Beveiliging banktransacties
KAS BANK N.V.

UNIVERSITEIT VAN AMSTERDAM

Auteurs	Bart Dorlandt	449725
	Carlos Groen	476854
In opracht van	KAS BANK N.V.	
	Universiteit van Amsterdam	
Begeleider	Martien Arends	

Versie	1.2 final
Datum	1 juli 2005

Management Overview

KAS BANK N.V. wil graag op een veilige manier online inzage en transactiediensten aanbieden. Hiertoe is een goede beveiliging noodzakelijk op het gebied van authenticatie, vertrouwelijkheid, integriteit en onweerlegbaarheid. Wij hebben hier onderzoek naar gedaan waarbij we ook gekeken hebben naar voorstellen van een aantal andere partijen. Hieruit zijn een aantal knelpunten naar voren gekomen die met name betrekking hebben op het gebrek aan controle over de klantomgeving.

Wij stellen voor een eigen systeem te plaatsen bij de klant, de KasBox. Deze KasBox is voorzien van alle benodigde functionaliteit voor zowel inzage als transacties en is volledig onder controle van KAS BANK N.V.: het is voor de klant niet mogelijk hierop software te installeren. De KasBox bouwt een beveiligde verbinding op over het internet en biedt daarnaast de mogelijkheid om uit te wijken naar de telefoonlijn. Met behulp van, op de smartcard opgeslagen, certificaten kunnen gebruikers zich authenticeren en toegang krijgen tot KasWeb. Transacties kunnen worden voorzien van een digitale handtekening waardoor onweerlegbaarheid verkregen wordt.

De KasBox is door het gebrek aan bewegende onderdelen zeer ongevoelig voor onderhoud, updates kunnen geautomatiseerd en op afstand plaatsvinden zodra de KasBox verbinding maakt met de server van KAS BANK N.V. Hierdoor is de KasBox ten allen tijden voorzien van de laatste updates en patches en is de vraag naar support minimaal.

Om de KasBox te realiseren is het nodig dat er een projectgroep wordt opgericht die de KasBox verder gaat ontwikkelen. Wij schatten dat er binnen een half jaar een werkbare versie moet zijn die op beperkte schaal kan worden uitgerold. Hierbij speelt de mogelijkheid van het op afstand updaten een grote rol doordat de ontwikkeling gewoon door kan gaan.

De kosten van onze oplossing zijn vergelijkbaar met de voorstellen van de andere partijen, waarbij opgemerkt dient te worden dat het een deeloplossing betreft: de uitgifte en het beheer van de certificaten is hierin niet meegenomen. Een groot deel van de kosten is eenmalig in verband met de ontwikkeling en de aanschaf van hardware. De kosten voor software zijn verwaarloosbaar omdat er gebruik wordt gemaakt van open-source oplossingen en eigen geschreven applicaties. In de volgende tabel zijn de verschillende kostenposten opgenomen voor de eerste 3 jaar (uitgaande van 500 KasBoxen):

	Kosten (euro)
Jaar 1	377.500
Jaar 2	120.000
Jaar 3	90.000
Totaal over 3 jaar	737.500

Inhoudsopgave

1 Inleiding

In het kader van de afsluiting van onze Masterstudie Systeem en Netwerkbeheer aan de Universiteit van Amsterdam hebben wij, Bart Dorlandt en Carlos Groen, een researchproject van een maand gedaan binnen de KAS BANK N.V. (vanaf nu afgekort tot KAS BANK). De KAS BANK heeft ons benaderd met het verzoek onderzoek te doen naar het bieden van een veiligde infrastructuur voor het online inzien van betalingsgegevens en het doen van online transacties. Het resultaat van dit onderzoek is een gedegen advies met betrekking tot een te implementeren infrastructuur, dat in dit document zal worden uitgewerkt. Daarbij richten we ons vooral op de technische aspecten en in mindere mate op de procedures met betrekking tot de uitgifte en het beheer van certificaten.

1.1 Kader

De KAS BANK

De KAS BANK is opgericht in 1806 en is een solide, gespecialiseerde Europese bank met een breed scala aan modulaire effecten- en informatiediensten. De dienstverlening is zowel gericht op institutionele beleggers, (pensioenfondsen en verzekeringsmaatschappijen) als op andere banken en commissionairs.

De kernactiviteiten van KAS BANK zijn custody, clearing en settlement. Vanuit deze nagenoeg volledig geautomatiseerde kerndienstverlening is een rijk geschakeerd palet aan afgeleide diensten ontwikkeld. Deze diensten bieden de afnemers ervan echte toegevoegde waarde; door ze werk uit handen te nemen, processen beter, sneller en goedkoper te laten verlopen en hun ondernemingen beter bestuurbaar te maken. Vooral de Investment Management Services voor professionele eindbeleggers ontwikkelen zich tot een core-service van de bank.

Naast neutraliteit en onafhankelijkheid onderscheidt de bank zich door het leveren van hoge kwaliteit, door professionele, kundige mensen, middels hoogwaardige robuuste technologie, waardoor cliënten echte toegevoegde waarde ervaren. KAS BANK biedt continuïteit en betrouwbare dienstverlening vanuit een financieel solide basis. Hiervoor gaf Standard & Poor's KAS BANK de A/Stable/A-1 rating.

Master Systeem en Netwerkbeheer

De master Systeem- en netwerkbeheer is een intensieve eenjarige opleiding van de Universiteit van Amsterdam (UvA), in samenwerking met de Hogeschool van Amsterdam (HvA). Met deze master specialiseer je je in systeem- en netwerkbeheer. Dat is een boeiend vak want systeem- en netwerkbeheerders spelen een centrale rol in het efficint en effectief functioneren en innoveren van een belangrijk deel van de technische infrastructuur van Nederland, namelijk computers, software en netwerken. De functionaliteit, het gebruik en de economische impact van deze infrastructuur neemt snel toe. De afhankelijkheid, de complexiteit en de gevaren van misbruik en mismanagement echter ook. Goed beheer vergt

mensen die zeer vertrouwd zijn met enerzijds het technisch detail en anderzijds met de doelstellingen en behoeften van organisaties en de maatschappij.

1.2 Probleemstelling

KAS BANK maakt op dit moment gebruik van een token-based systeem om klanten toegang te bieden tot hun online diensten in de vorm van KasWeb. Dit systeem is ontworpen ten behoeve van inzage functies en kleine transacties. KAS BANK wil de mogelijkheid bieden om op een veilige manier via KasWeb zowel grote als kleine transacties te doen. Het huidige systeem voldoet niet aan de beveiligingseisen die de KAS BANK hieraan stelt.

Daarom is gekeken naar een aantal mogelijke oplossingen waarbij aan diverse veiligheidsaspecten wordt voldaan en waarbij de te leveren support voor de KAS BANK minimaal is. Deze oplossingen zijn erg prijzig en laten, met name aan de kant van de gebruiker, ruimte voor verbetering.

1.3 Doelstelling

Vanuit de theorie komen tot een gedegen advies met betrekking tot een veilige infrastructuur voor communicatie tussen klanten en de KAS BANK. Hierbij ligt de nadruk op het kunnen aanbieden van de mogelijkheid veilig online transacties te doen (klein en groot). Eerste prioriteit hierbij is veiligheid, waarbij gelet dient te worden op: *authenticatie, vertrouwelijkheid, integriteit* en *onweerlegbaarheid*, daarna komen onderhoudbaarheid, kosten en gebruikersgemak.

1.4 Scope

De scope van dit onderzoek is:

- Beveiligde communicatie op basis van een Public Key Infrastructure
- Het beveiligen van de omgeving van de klant
- Het beveiligen van de omgeving van de server (globaal)

Niet:

- Specifieke applicaties
- Uitgifte en beheer van certificaten
- Procedures

1.5 Opbouw van het document

Allereerst worden een aantal relevante begrippen met betrekking tot beveiliging genoemd en uitgelegd. Vervolgens geven we een omschrijving van de huidige en gewenste situatie en vatten we kort de voorstellen van een aantal andere partijen samen. Hierop analyseren we de gewenste situatie en de voorgaande voorstellen waaruit een aantal knelpunten met betrekking tot de beveiliging naar boven komen. Hierop baseren we vervolgens onze oplossing die wordt gevolgd door een dreigingenanalyse en een haalbaarheidsstudie. We sluiten af met onze aanbevelingen en een paar discussiepunten.

2 Begrippenkader

Ter verduidelijking van de in dit document genoemde termen en methoden wordt in dit deel kort uitgelegd wat de begippen inhouden en hoe ze toegepast worden.

2.1 Betrouwbaarheid van informatie

Informatie vormt de kern van de dienstverlening van de KAS BANK. Richting de klant is dit informatie over eerdere gedane transacties en de status van lopende transacties, richting de KAS BANK is zijn dit de transacties zelf. Deze informatie dient betrouwbaar te zijn en derhalve beschermd te worden tegen zowel opzettelijk als onopzettelijk foutief handelen. Daartoe zijn de volgende begrippen gedefiniërd:

Beschikbaarheid: Beschikbaarheid is het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

Integriteit: Integriteit is het waarborgen van de correctheid en de volledigheid van informatie en verwerking.

Vertrouwelijkheid: Vertrouwelijkheid is het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Onweerlegbaarheid: Onweerlegbaarheid is het principe dat niet weerlegd kan worden dat men verantwoordelijk is voor een bepaalde daad.

Authenticatie: Authenticatie is de verificatie van de identiteit van een partij. Het garandeert de identiteit van diegene met wie gecommuniceerd wordt.

2.2 Cryptografie

Cryptografie is de wetenschap van het omzetten van informatie van leesbare naar onleesbare vorm. Bij dit proces wordt de informatie dusdanig versleuteld dat het slechts leesbaar is voor de partij waarvoor het bedoeld is. Hiertoe wordt gebruikgemaakt van een encryptiealgoritme en een sleutel. De versleutelde informatie kan onderschept worden maar zonder bijbehorende sleutel is het niet mogelijk de informatie te lezen of te wijzigen.

Sleutels: Een sleutel is een unieke waarde waarmee een bericht verleuteld wordt. Bij symmetrisch versleuteling wordt dezelfde sleutel gebruikt voor het versleutelen en het ontsleutelen, bij asymetrische versleuteling wordt een sleutel gebruikt voor versleuteling en een andere voor ontsleuteling.

PKI: PKI staat voor Public Key Infrastructure. Het is een systeem gebaseerd op asymmetrische versleuteling waarbij de ene sleutel de publieke sleutel

wordt genoemd en de andere sleutel de private sleutel. De publieke sleutel is wordt bekend gemaakt, de private sleutel wordt geheim gehouden. Een bericht dat met de publieke sleutel wordt versleuteld is alleen te lezen met behulp van de bijbehorende private sleutel, een bericht dat met de private sleutel wordt versleuteld is alleen te lezen met de publieke sleutel. Dit toont aan dat degene die het bericht versleuteld heeft de eigenaar is van deze sleutel.

Signeren: de digitale handtekening: Het signen van een bericht, het zetten van een digitale handtekening, gebeurt door een unieke verkorte versie van het bericht te versleutelen met de private sleutel. Het maken van deze verkorte versie gebeurt door middel van een algoritme dat hashing heet. Hierbij wordt een checksum van het bericht gecreëerd die (vrijwel) uniek is voor dat bericht. Wijzigt het bericht dan wijzigt deze checksum. Door deze checksum te versleutelen met de private sleutel en vervolgens mee te sturen met het bericht wordt de integriteit van het bericht gewaarborgd evenals de identiteit van de afzender. Omdat de afzender de enige is die weet heeft van de private sleutel waarmee het bericht gesigned is wordt ook onweerlegbaarheid verkregen.

Certificaten: Een certificaat is als een creditcard. Het bevat o.a. je naam, een uniek serienummer en een tweetal data. De eerste datum geeft aan wanneer het certificaat is uitgegeven en de andere datum is tot wanneer het certificaat geldig is. Daarnaast bestaat uit je eigen unieke sleutelpaar, een private en publieke sleutel. Deze zijn gesigneerd door de uitgever, de Certification Authority. Hieruit is af te leiden dat het certificaat "echt" is.

Een standaard voor de certificaten is de X.509 (pag 391 [2]).

Certification Authority: Een CA (Certification Authority) kan voor de KAS BANK een externe partij zijn welke de sleutels creëerd, signeerd en uitdeelt. Hierdoor is er geen extra belasting voor de KAS BANK. De CA beheerd de sleutels voor de KAS BANK en de klanten van de KAS BANK. Het kan een revocation list bijhouden van de sleutels die bijvoorbeeld gestolen zijn. Hierdoor kan een gestolen sleutel later niet opnieuw gebruikt worden.

Deze CA zal gekoppeld worden aan het systeem van de KAS BANK. Hierdoor zouden zogenaamde ACLs (Access Control List) gemaakt kunnen worden op basis van de sleutel. Hiermee kan toegang verleend worden aan bepaalde sleutels (personen).

Ook is het mogelijk om gebruik te maken van RBAC (Role Based Access Control). Hiermee is het mogelijk om een bepaalde persoon gebruiker maar ook administrator te laten zijn, afhankelijk van de manier waarop hij/zij inlogt.

TTP: Een Trusted Third Party (TTP) is zoals de naam aangeeft; een derde partij die te vertrouwen is. Een TTP heeft weet van publieke sleutels van

aangesloten partijen. Het komt ook voor dat de TTP zelf sleutelparen (digitale handtekeningen) uitgeeft Op deze manier kan de TTP garanderen dat een sleutel bij een bepaalde persoon hoort. Hoe de TTP op de andere manier de juiste publieke sleutel ontvangt is procedureel vastgelegd.

Wanneer klant A een gesigneerd bericht verstuurd (gesigneerd met de private sleutel) naar klant B weet klant B niet of het klant A is die het bericht heeft gestuurd (Klant B weet de publieke sleutel van klant A nog niet). Aangezien de TTP wel de juiste publieke sleutel heeft, kan de TTP bevestigen aan klant B dat dit bericht echt door klant A verstuurd is.

Smartcards: Smartcards zijn tamper-free devices waarin certificaten kunnen worden opgeslagen. Deze certificaten kunnen niet worden uitgelezen maar informatie kan naar de smartcard worden verstuurd waarna deze door de smartcard kan worden ver- of ontsleuteld. Hiervoor is het nodig dat er een smartcard-reader aan het betreffende systeem is gekoppeld.

2.3 VPN

Met een Virtual Private Network (VPN) is het mogelijk een veilige verbinding op te zetten over een onveilig medium. Dit kan onder andere door middel van IPSec of SSL/TLS. Beide methoden zijn gebaseerd op PKI. Wanneer een VPN opgezet wordt, wordt gecommuniceerd over een tunnel. Deze tunnel is een end tot end verbinding waar niemand kan afluisteren. Voor de gebruiker lijkt het op deze manier alsof hij/zij zich in het andere netwerk bevindt.

IPSec: IPSec is een set van protocollen ontwikkeld door de IETF (Internet Engineering Task Force) om pakketten veilig over te sturen. Deze protocollen werken op de IP laag. (laag3)

IPSec wordt gebruikt voor transport en voor tunnels. Bij transport wordt alleen het dataveld in het pakket versleuteld en bij tunnels wordt de header en het dataveld versleuteld.

SSL: Secure Sockets Layer (SSL) werkt op laag 4 van het OSI model en gebruikt voor de communicatie het TCP protocol. SSL wordt gebruikt voor het versleutelen van verkeer en het authenticeren. Bij normaal webgebruik wordt de server geauthenticeerd aan de hand, in de client opgeslagen, root certificaten. Voor de communicatie zoals die in dit document wordt beschreven wordt gebruik gemaakt van wederzijdse communcatie aan de hand van zowel server als client certificaten. De gebruikte SSL versie is versie 3.

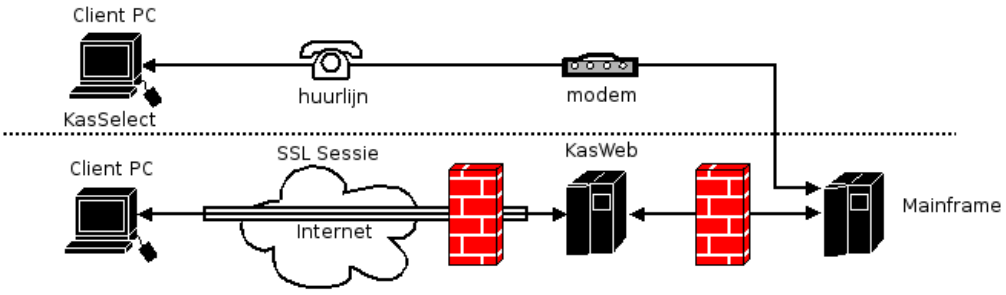
Het opzetten van een SSL verbinding gebeurt middels een handshake tussen de client en de server. Hierbij wordt een encryptieprotocol afgesproken en worden certificaten en een aantal random nummers uitgewisseld. Uit deze nummers worden een zestal session keys (drie voor verzending en 3 voor ontvangst) berekend die voor de duur van de sessie gebruikt worden om het verkeer te versleutelen. Aan de hand van de uitgewisselde certificaten kunnen de beide partijen elkaar authenticeren.

TLS: Transport Layer Security (TLS) is de opvolger van SSL. Ondanks dat TLS zijn eigen versie nummer, nummer 1.0, heeft, is het ook bekend als SSL versie 3.1. Door de IETF is er weinig gewijzigd, maar ondanks dat kunnen deze twee versie niet met elkaar kunnen communiceren. De wijzigingen die zijn gemaakt zijn onder andere, meer waarschuwingsberichten en aanpassingen in de computatie van de versleuteling.

F5 server: De F5 server is een application gateway waarnaar gebruikers op een veilige manier toegang kunnen krijgen tot hun bedrijfsnetwerken via een web browser. Hiervoor hoeven geen aanpassingen gemaakt te worden aan de computers van de gebruikers. De verbinding die wordt aan gegaan wordt beveiligd op basis van SSLVPN.

De F5 heeft een ingebouwde database waarmee het de ingevoerde gegevens met wachtwoorden controleert. Tevens is het mogelijk om de F5 aan een bestaande RADIUS of LDAP omgeving te koppelen. Het ondersteunt ook de mogelijkheid om aan te loggen door middel van een RSA SecurID of een VASCO Digipass.

3 Huidige situatie



Figuur 1: huidig netwerk

3.1 Gebruikers

KAS BANK levert inzage en transactiediensten aan 150 klanten met in totaal ongeveer 1500 gebruikers. Het aantal gelijktijdige gebruikers ligt ongeveer tussen de 150 en 200.

3.2 Informatiestromen

De informatiestromen tussen de klant en de KAS BANK zijn globaal in te delen in twee categorieen: inzage en transacties.

Inzage betreft het opvragen van gegevens over lopende en gedane beleggingen en betalingen. Deze gegevens kunnen worden gebruikt om overzichten en rapporten te genereren of om bijvoorbeeld de status van transacties te controleren. Dit kan zowel offline als online.

Transacties betreft het geven van instructies met betrekking tot betalingen en levering van effecten. Hiertoe behoort ook de bevestiging door anderen. Dit gebeurt, afhankelijk van de werkwijze van de klant, per transactie of enkele malen per dag in batchvorm. Hierbij gaat het om bedragen variërend van enkele honderden tot enkele miljoenen euro's.

3.3 Applicaties

Er zijn momenteel twee applicaties in gebruik die beide inzage en transactiefunctionaliteit bieden. Het eerste systeem heet KasSelect en werkt op basis van Foxpro. Dit pakket is bij de klant geïnstalleerd. Hiermee is de klant in staat offline overzichten te genereren en transacties aan te maken. Deze transacties worden verzameld en verstuurd zodra er weer contact wordt gemaakt met de KAS BANK. Beveiliging is gebaseerd op beveiliging van de infrastructuur. Er is geen limiet gesteld aan de hoogte van de transacties.

Het andere systeem is KasWeb. Dit is een webbased applicatie waarmee klanten middels een standaard webbrowser online inzage hebben in hun gegevens. Er is geen sprake van offline opslag waardoor gegevens altijd up to date zijn. Dit vormt wel een zware belasting op de webserver van de KAS BANK. Het is met dit systeem ook mogelijk om transacties te doen. Hierbij worden transacties van een digitale handtekening voorzien met behulp van een VASCO DigiPass 3000. De hoogte van de transacties is gelimiteerd op 10.000 euro.

3.4 Infrastructuur

Communicatie tussen de klant en de KAS BANK verloopt via verschillende media. Voor de genoemde applicaties, KasSelect en KasWeb, is dit over respectievelijk dedicated verbindingen (zoals huurlijnen) en het internet. Verder worden transacties veelal nog bevestigd over traditionele media als de telex, de fax, de telefoon en de post.

De KasWeb server bevindt zich in de DMZ (DeMilitarized Zone) (figuur 1) en is direct bereikbaar vanaf het internet. Hierbij maakt elke gebruiker van KasWeb via de browser contact met deze server. Deze server maakt vervolgens verbinding met het mainframe binnen het interne KAS BANK netwerk. KasSelect gebruikers maken via de huurlijn direct verbinding met het mainframe.

4 Gewenste situatie

In de gewenste situatie is het voor klanten mogelijk om online gebruikt te maken van de diensten van de KAS BANK. Hiervoor is een goede beveiliging benodigd die minstens van hetzelfde niveau is als de oplossing van SWIFT maar een stuk eenvoudiger en goedkoper is. Er moet rekening worden gehouden met ten minste 5000 gebruikers. In het ideale geval is de nieuwe situatie schaalbaar naar een grotere groep gebruikers en/of medewerkers.

De huidige KasSelect applicatie wordt uitgefaseerd. Omdat KasSelect vaak is geïntegreerd in de bestaande informatiesystemen bij de klant moet er een oplossing komen waarbij de functionaliteit behouden blijft. Dit valt buiten de scope van dit rapport. Klanten die alleen inzage wensen kunnen voorlopig nog gebruik maken van KasWeb. Hieruit verdwijnt de transactiefunctionaliteit: deze wordt alleen aangeboden via de nieuw te implementeren beveiligde infrastructuur.

In eerste instantie wordt de gewenste situatie een veilig communicatiemedium waarover grote transacties gegarandeerd veilig verstuurd kunnen worden. Later kan dezelfde infrastructuur mogelijk ingezet worden voor andere beveiligde diensten, bijvoorbeeld email. In eerste instantie zal alleen toegang vanaf de locatie van de klant mogelijk zijn. Hierna kan gekeken worden naar flexibelere oplossingen omtrent inzage, maar ook transacties tot een bepaald bedrag.

Door de KAS BANK is aangegeven dat een F5 machine beschikbaar is voor de beveiliging en dat het voorkeur heeft deze te gebruiken. Voor het beheer van de gebruikers wenst KAS BANK gebruik te maken van een Active Directory systeem.

4.1 Requirements

Onderstaande de requirements zoals aangegeven door de Kasbank in willekeurige volgorde. Deze requirements zijn van toepassing op de eerder genoemde te realiseren infrastructuur.

- De te ontwerpen infrastructuur dient te voldoen aan de beveiligingseisen op basis van authenticatie, vertrouwelijkheid, integriteit en onweerlegbaarheid
- De te ontwerpen infrastructuur dient alleen gebruik vanaf een vaste, vooraf gedefinieerde, locatie te faciliteren.
- De te ontwerpen infrastructuur dient, naast voor transacties, ook voor andere diensten gebruikt te kunnen worden.
- De te ontwerpen infrastructuur dient naast de bestaande infrastructuur geïmplementeerd te kunnen worden.
- De te ontwerpen infrastructuur dient gebruiksvriendelijk te zijn en door de klant te installeren te zijn.

- De te ontwerpen infrastructuur dient minimale support te vereisen.
- De te ontwerpen infrastructuur dient gemakkelijk te onderhouden te zijn.

5 Voorgaande voorstellen

Vier partijen zijn door KAS BANK verzocht een voorstel te doen voor een veilige infrastructuur voor transacties. Deze voorstellen worden hier kort beschreven en de globale kosten worden genoemd.

5.1 SWIFT

SWIFT is een bekende partij binnen de bankwereld en biedt een complete oplossing over een bestaande veilige infratructuur genaamd SWIFTnet. Deze infrastructuur bestaat uit VPN verbindingen over een beveiligd stand-alone netwerk. Authenticatie gebeurt op basis van werkplek en middels een PKI, waarbij een klant (niet een gebruiker !) zich authenticeert met een smartcard. Transacties worden voorzien van een digitale handtekening door zowel de klant als door SWIFT. Over SWIFTnet kan een klant meerdere diensten afnemen waaronder communicatie met andere SWIFT gebruikers. Hiervoor wordt door SWIFT bij de klant een systeem geplaatst en worden procedures opgelegd om dit systeem te beschermen. Niet alleen de KAS BANK dient te zijn aangesloten op SWIFT, maar ook alle klanten die over het SWIFT netwerk met de KAS BANK willen communiceren. Hiervoor moeten zij in principe ook klant worden van SWIFT of "Participant Member" van een speciale "closed user group" van de KAS BANK.

Klant worden van SWIFT is erg complex en duur. Een bedrijf moet aan hoge eisen voldoen met betrekking tot beveiliging en bedrijfsvoering. Het worden van "Participant Member" is iets eenvoudiger en goedkoper maar nog steeds aan veel regels gebonden.

5.2 Partij U

Het voorstel van partij U heeft voornamelijk betrekking op het implementeren van een PKI binnen de KAS BANK. Deze PKI is breed inzetbaar voor zowel transacties als het bijvoorbeeld het versleutelen en signeren van E-mails en het authenticeren van andere applicaties. Hierbij is sprake van een softwareoplossing bij de klant en wordt gebruik gemaakt van smartcards met certificaten voor de authenticatie van gebruikers. Deze certificaten worden door partij U zelf uitgegeven en beheerd middels een Certificate Authority. De technische implementatie wordt verder in het midden gelaten.

5.3 Partij R

Het voorstel van partij R beschijft een oplossing op basis van PKI met software op het systeem van de klant. Er wordt directe communicatie over het internet voorgesteld tussen de browser van de klant en de KasWeb server waarbij gebruik wordt gemaakt van webservices op basis van Soap/XML. Hierbij vindt authenticatie en versleuteling plaats op basis van SSL met wederzijdse certificaten. Transacties worden online voorzien van een digitale handtekening met

behulp van applet of plugin of offline via een JAVA of .NET applicatie waarbij diverse smartcard-readers gebruikt kunnen worden. Deze handtekening wordt geverifiëerd door een webservice die communiceert met een LDAP oplossing.

De uitgifte van certificaten wordt uitbesteed aan een derde partij.

5.4 Partij A

Partij A stelt ook een oplossing op basis van PKI voor met software op het systeem van de klant. Deze oplossing lijkt erg op die van Partij R. Als verschil kan worden aangemerkt dat partij A specifiek aangeeft uit te gaan van 2 verschillende certificaten: een voor de verbinding en een voor het signen. Verder wordt er uitgegaan van een Active Directory server en is de implementatie bij de klant gebaseerd op een Microsoft crypto API. Hierdoor worden meer verschillende smartcard-readers ondersteund dan bij de oplossing van Partij R.

Certificaten worden op de smartcard gegeneereerd waardoor er geen externe partij nodig is.

6 Analyse

In dit deel worden aan de hand van de requirements gekeken naar de voorgaande voorstellen en worden knelpunten gezocht. Aan de hand van deze analyse wordt in de volgende delen een oplossing uitgewerkt.

Het beveiligingsmodel bestaat uit de volgende onderdelen:

- Een PKI voor authenticatie en het signen van de transacties.
- Een beveiligde verbinding.
- Een beveiligde omgeving bij de klant: De KasBox.
- Een beveiligde omgeving bij de KAS BANK.
- Procedures voor gebruik.

6.1 PKI

De basis van het beveiligingsmodel wordt gevormd door een PKI systeem. Alle andere partijen baseren hun voorstellen hierop en ook branchegenoten gebruiken een PKI voor hun authenticatie en beveiliging. Een PKI blijkt te voorzien in alle eisen die gesteld worden op het gebied van authenticatie, vertrouwelijkheid, integriteit en onweerlegbaarheid:

	Authenticatie	Vertrouwelijkheid	Integriteit	Onweerlegbaarheid
Private Network	Ja (werkplek)	Ja	Ja	Nee
VPN	Ja (werkplek)	Ja	Ja	Nee
PKI/Smartcard	Ja	Ja	Ja	Ja

De PKI implementatie die wordt voorgesteld bestaat uit een smartcard met daarop een of meerdere certificaten. De certificaten kunnen niet worden gelezen van de smartcard maar gegevens worden in de, op de smartcard aanwezige chip, gecodeerd en gedecodeerd.

6.1.1 Authenticatie

Authenticatie van een persoon is gestoeld op de volgende drie principes:

1. What you know
2. What you have
3. What you are

Een sterke authenticatie is gebaseerd op minstens twee van deze principes. Vaak wordt een combinatie van 1 en 2 gebruikt waarbij een certificaat op een smartcard wordt ontsloten door een wachtwoord dat alleen aan de gebruiker bekend

is. Dit biedt een redelijke mate van beveiliging. Toch zijn hieraan nog gevaren verbonden. Zo kan met behulp van een keylogger of door het meekijken bij het invoeren het wachtwoord informatie worden achterhaald.

Een nog sterkere authenticatie wordt bereikt door hieraan een biometrische component toe te voegen, waarbij een gebruiker een certificaat ontsluit met behulp van zijn vingerafdruk eventueel nog in combinatie met een wachtwoord. Hiervoor zijn speciale smartcard-readers beschikbaar met ingebouwde fingerprint scanner.

De KAS BANK heeft aangegeven dat zij een beveiliging op basis van de eerste twee principes voldoende acht.

6.1.2 Aantal certificaten

Voor de authenticatie van een gebruiker is in theorie een enkel certificaat voldoende. Dit certificaat kan dienen voor zowel toegang en inzage als het signen van transacties. Hierbij is de vraag wanneer het bijbehorende wachtwoord ingevoerd dient te worden. Als dit eenmalig wordt ingevoerd bij het verbinden dan kan een ander transacties doen als de gebruiker van het systeem weg is. Als het om de paar minuten moet worden ingevoerd dan maakt dit het systeem erg ongebruiksvriendelijk. Een oplossing hiervoor is het gebruik van meerdere certificaten met elk een eigen wachtwoord: een voor inzage en een voor transacties. Omdat inzage minder gevoelig is kan het wachtwoord hiervoor eens per sessie worden ingevoerd of na een bepaalde periode van inactiviteit. Het wachtwoord voor transacties moet vervolgens voor elke transactie of verzameling van transacties worden ingevoerd.

6.1.3 Uitgifte van certificaten

Het principe van onweerlegbaarheid is gebaseerd op het feit dat de beide partijen geen weet hebben van elkaars private sleutel. Om te kunnen bewijzen dat een transactie is gedaan door de gebruiker mag de KAS BANK dus niet in het bezit zijn van diens certificaat. Hierdoor zou uitgifte dus moeten gebeuren door een derde vertrouwde partij.

Omdat de KAS BANK een bank is kan hiervan worden afgeweken. Hierbij dient de KAS BANK aannemelijk te maken dat de uitgifte is gebeurd door een geheel andere afdeling dan degene die de transacties afhandelt: het zogenaamde Chinese Wall principe.

Een andere oplossing is het genereren van het certificaat op de smartcard waarbij het certificaat, en dus de private sleutel, de smartcard nooit verlaten: alleen de publieke sleutel kan worden uitgelezen. Hierbij is het dus niet nodig om de uitgifte van certificaten door een derde partij te laten doen om onweerlegbaardheid te verkrijgen.

6.1.4 Certificate Authority

Alle communicatie vindt direct plaats tussen de klant en de KAS BANK waardoor het signen van het certificaat door een derde partij, met als doel het verzekeren van de echtheid van het certificaat, overbodig is.

6.2 Verbinding

Voor de communicatie tussen de klant en de KAS BANK is een beveiligde verbinding nodig. Hiervoor voldoet een VPN oplossing over het internet. Hierbij kan gekozen worden tussen de meest gangbare VPN implementaties IPSec en SSL. Beide protocollen kunnen gebruik maken van certificaten en bieden een hoogwaardige beveiliging, waarbij IPSec als eigenschap heeft dat het standaard het gehele interne netwerk ontsluit terwijl SSL specifiek een tunnel voor een bepaalde toepassing biedt. Beide protocollen bieden, mits goed geconfigureerd, de benodigde functionaliteit.

De voorgaande voorstellen houden geen rekening met het uitvallen of niet beschikbaar zijn van een internetverbinding. Met het oog op de continuïteit en de tijdgebondenheid van transacties is het verstandig hier rekening mee te houden en te voorzien in een uitwijkvoorziening.

6.3 Omgeving klant

Uit de voorgaande voorstellen blijkt dat, op het voorstel van SWIFT na, in alle gevallen gekozen is voor een software-oplossing op een systeem van de klant. De KAS BANK heeft aangegeven hieraan de voorkeur te geven in verband met de vraag naar support bij een, door KAS BANK geleverde, hardwareoplossing.

Toch brengt een software-oplossing een aantal veiligheidsrisico's met zich mee. Het besturingssysteem is mogelijk niet veilig geconfigureerd en van de laatste beveiligingsupdates voorzien waardoor het kwetsbaar is voor hackers of malware zoals virussen, worms, trojan horses. Daarnaast wordt het systeem mogelijk nog gebruikt voor andere doeleinden waardoor de mogelijkheid bestaat dat er opzettelijk of onopzettelijk malware of keyloggers op worden geïnstalleerd.

Malware kan een kwaadwillende controle over het systeem geven waarbij gegevens worden onderschept en ongemerkt wijzigingen worden uitgevoerd. Zo is het theoretisch mogelijk dat een transactie wordt gedaan met een ander bedrag of naar een andere partij dan op het scherm staat.

Vanuit het oogpunt van veiligheid is het raadzaam om te kijken naar een oplossing waarbij er voor de KAS BANK volledige controle bestaat over het systeem van de klant. Dit is mogelijk door software te installeren die het gehele systeem overneemt (zoals DNB doet) of door het plaatsen van eigen hardware met alle benodigde software voorgeïnstalleerd. Dit laatste heeft de volgende voordelen:

- Het systeem kan niet besmet zijn met een virus, worm of trojan horse voorafgaande aan de installatie van de software.

- Het systeem is voorzien van de laatste beveiligingsupdates en patches en veilig geconfigureerd.
- De klant hoeft geen software meer te installeren en er kunnen geen fouten worden gemaakt bij de installatie.
- Er hoeft geen rekening te worden gehouden met compatibiliteit met hardware van de klant, zowel bij installatie als bij updates.
- De klant hoeft geen extra licenties aan te schaffen en geen extra hardware te kopen.

Een hardwareoplossing bij de klant brengt ook een aantal problemen met zich mee. KAS BANK is verantwoordelijk voor de juiste werking van het systeem. Hierbij zal de klant, in het geval van problemen met de hardware, aanspraak maken op support. Onderhoud en updates moeten gemakkelijk kunnen worden uitgevoerd en het moet mogelijk zijn het systeem op afstand te kunnen monitoren. Er moet worden nagedacht over klantomgevingen waarbij er meerdere werkplekken zijn waarvandaan transacties worden gegenereerd, bijvoorbeeld trading rooms. Hierbij is een bijkomend probleem dat er vaak beperkte ruimte is op de werkplek waarbij er geen ruimte is voor extra monitoren en/of toetsenborden. Ook kan het zijn dat klanten terughoudend zijn over het plaatsen van vreemde hardware in hun netwerk.

6.4 Omgeving KAS BANK

Voor het opzetten van een beveiligde verbinding tussen de klant en de KAS BANK is reeds een F5 server aanwezig bij de KAS BANK. Deze F5 biedt alle benodigde functionaliteit voor het opzetten van een VPN verbinding en het authenticeren middels certificaten.

Voor de authenticatie van gebruikers heeft KAS BANK aangegeven gebruik te willen maken van een Active Directory systeem. Hierin kunnen de gebruikers worden beheerd en hun publieke sleutels worden opgeslagen.

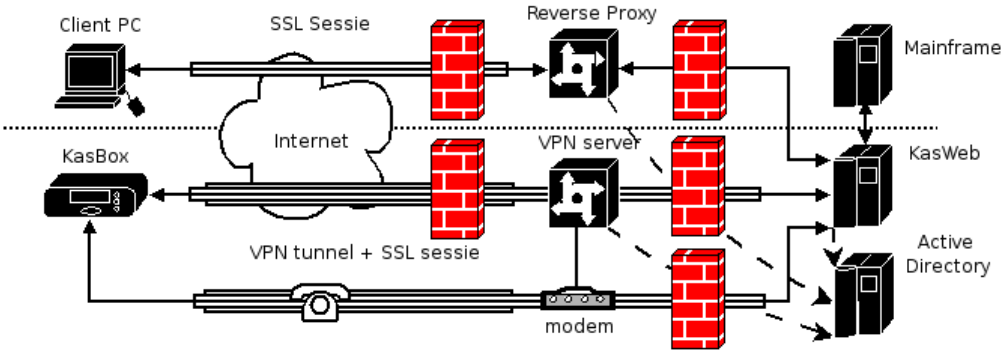
Op applicatieniveau wordt gebruik gemaakt van de reeds aanwezige KasWeb server. Naast over de te bieden beveiligde infrastructuur moet ook nog gebruik kunnen worden gemaakt van inzagefunctionaliteit over het internet.

6.5 Procedures

In procedures moet voornamelijk worden vastgelegd hoe de distributie van certificaten verloopt, hoe smartcards en hardware dienen te worden opgeslagen en hoe wordt omgegaan met diefstal van smartcards etc.

7 Onze oplossing

In de analyse hebben we aangegeven dat een oplossing waarbij de KAS BANK de volledige controle over het systeem van de klant heeft het veiligste is. Ook hebben we een aantal voordelen en aandachtspunten genoemd van een, door de KAS BANK geleverde, hardwareoplossing. In dit deel werken we een dergelijke oplossing (de KasBox) uit waarbij we ook ingaan op de genoemde aandachtspunten. We geven een implementatie van een PKI, een verbinding gebaseerd op VPN en een voorstel voor de KAS BANK omgeving. We sluiten af met een summiere opsomming van procedures die hierbij van belang zijn.



Figuur 2: nieuw netwerk

7.1 PKI

Er wordt gebruik gemaakt van een drietal certificaten bij de gebruiker: een certificaat op de KasBox en een tweetal certificaten op een smartcard. Deze certificaten bevatten de geheime sleutels van de gebruiker alsmede een publieke sleutel van de KAS BANK. De bijbehorende geheime sleutel van de KAS BANK is (uiteraard) alleen aan de KAS BANK bekend. In tabelvorm ziet dit er als volgt uit:

Certificaat	Locatie	Versleuteld	Sleutels klant	Sleutels KAS
Cert A	KasBox	Met K_{priv}	KA_{priv}, K_{pub}	KA_{pub}, K_{priv}
Cert B	Smartcard	Met wachtwoord P_B	KB_{priv}, K_{pub}	KB_{pub}, K_{priv}
Cert C	Smartcard	Met wachtwoord P_C	KC_{priv}, K_{pub}	KC_{pub}, K_{priv}

Voor elk certificaat heeft de KAS BANK een publieke sleutel opgeslagen in de eigen (Active Directory) database. Hiermee kan de KAS BANK de gebruiker middels zijn certificaten authenticeren. Op het moment dat een nieuw certificaat wordt aangemaakt wordt de bijbehorende publieke sleutel aan de betreffende gebruiker gekoppeld in de database, op het moment dat een certificaat

wordt ingetrokken (bijvoorbeeld in verband met diefstal) wordt deze sleutel in de database geblokkeerd (of verwijderd).

Certificaat A: verbinding Certificaat A is opgeslagen op de KasBox en is uniek voor die specifieke KasBox. Het certificaat is versleuteld met de private sleutel van de KAS BANK. Voor ontsleuteling is een smartcard nodig met daarop de publieke sleutel van de KAS BANK: hierdoor kan het alleen gelezen worden in combinatie met een geldige smartcard.

Op basis van de private sleutel in dit certificaat authenticeert de KasBox zich en wordt een beveiligde verbinding met de KAS BANK tot stand gebracht. De verbinding blijft bestaan zolang de smartcard in de smartcardreader zit.

Wordt de KasBox gestolen dan wordt de bijbehorende publieke sleutel geblokkeerd in de database van de KAS BANK en kan de KasBox niet meer worden gebruikt.

resultaat: beveiligde verbinding, authenticiteit (van de KasBox), vertrouwelijkheid, integriteit.

Certificaat B: sessie Certificaat B staat opgeslagen op de smartcard en is uniek voor de gebruiker. Het certificaat dient ontsloten te worden met een wachtwoord. Op basis van de private sleutel in dit certificaat authenticeert de gebruiker zich en wordt een sessie naar de KasWeb tot stand gebracht over de eerder opgebouwde beveiligde verbinding. De sessie blijft bestaan zolang de smartcard in de reader zit of wordt verbroken na een bepaalde periode van inactiviteit. Hierna dient een nieuwe sessie te worden gestart waarbij opnieuw het wachtwoord moet worden ingevoerd.

Wordt de smartcard gestolen dan wordt de bijbehorende publieke sleutel geblokkeerd in de database van de KAS BANK en kan het certificaat niet meer worden gebruikt.

resultaat: sessie waarmee inzage mogelijk is, authenticiteit (van de gebruiker), vertrouwelijkheid, integriteit.

Certificaat C: transactie Certificaat C staat opgeslagen op de smartcard en is uniek voor de gebruiker. Het certificaat dient ontsloten te worden met een wachtwoord. Een transactie of groep van transacties wordt met behulp van de private sleutel in dit certificaat voorzien van een digitale handtekening. Hiervoor is het nodig dat er reeds een sessie bestaat. Elke nieuwe transactie of groep van transacties dient voorzien te worden van een nieuwe digitale handtekening waarvoor elke keer het wachtwoord moet worden ingevoerd.

Wordt de smartcard gestolen dan wordt de bijbehorende publieke sleutel geblokkeerd in de database van de KAS BANK en kan het certificaat niet meer worden gebruikt.

resultaat: transactie voorzien van een digitale handtekening, authenticiteit (van de gebruiker), integriteit, onweerlegbaarheid.

7.2 Beveiliging

Het gebruik van een derde certifcaat op de KasBox dient als extra beveiliging. Hierdoor kan een smartcard niet los van een KasBox worden gebruikt en andersom is er een geldigde smartcard nodig om de KasBox te kunnen gebruiken. De combinatie van KasBox, smartcard en wachtwoord is nodig om verbinding te maken en een sessie te starten. Een apart certficiaat met een eigen wachtwoord is nodig voor het signen van de transacties. Eventueel kan gekozen worden voor biometrische ontsluiting in plaats van, of in combinatie met, een wachtwoord. Hiervoor kan in deze tekst in plaats van wachtwoord dan de vingerafdruk worden gelezen.

7.3 Verbinding

De verbinding met de KAS BANK is gebaseerd op een VPN oplossing over het internet waarbij wederzijdse authenticatie plaatsvindt op basis van de certificaten. Naast authenticatie worden deze certificaten ook gebruikt bij het uitwisselen van sessiesleutels voor versleuteling van de verbinding. Wij gaan uit van de SSL implementatie omdat dit het makkelijkst is te configureren en in principe even veilig is als de IPSec variant. Hierbij wordt een SSL tunnel opgebouwd vanuit de KasBox naar de VPN server bij de KasBank, de F5. Over deze tunnel wordt vervolgens de sessie opgebouwd die wederom, onafhankelijk van de VPN tunnel, versleuteld is. Mocht op de een of andere manier de VPN tunnel gecompromiteerd raken dan zorgt deze tweede versleuteling dat de data alsnog niet te lezen is.

Een uitwijkmogelijkheid wordt geboden in de vorm van een telefoonverbinding waarover, net als via het internet, een VPN verbinding wordt opgebouwd. Deze verbinding biedt dezelfde functionaliteit als een VPN verbinding over het internet al is hij welliswaar iets trager.

7.4 De klantomgeving: KasBox

De KasBox bevat alle benodigde functionaliteit voor inzage en het doen van transacties. Er kan over het internet of via de telefoonlijn verbinding worden gemaakt met KAS BANK en middels een grafische browser kan gebruik worden gemaakt van KasWeb. Met de bijgeleverde smartcard-reader kunnen de smartcards van gebruikers worden gelezen en de daarin opgeslagen certficaten worden gebruikt. Voor het signen van een transactie zou een Java Applet gebruikt kunnen worden.

De KasBox heeft de volgende eigenschappen:

- De behuizing is relatief klein: ca. 15 x 20 x 3 cm.
- De KasBox bevat geen bewegende delen: data opslag vindt plaats op een flash card.
- De KasBox is voorzien van een kleine en veilige linuxdistributie.

- De KasBox is eenvoudig op afstand te monitoren en te updaten.
- De KasBox is voorzien van aansluitingen voor zowel het netwerk als de telefoonlijn.
- De KasBox wordt geleverd inclusief (biometrische) smartcard-reader.

7.4.1 Beveiliging

Om de beveiliging van de KasBox te beschrijven geven we een aantal voorbeelden van aanvallen waarbij we aangeven hoe de KasBox hiertegen beschermd is.

Aanvallen vanaf het netwerk De KasBox heeft een ingebouwde firewall die alleen uitgaand VPN verkeer toestaat. Alle verbindingen worden geïnitialieerd vanuit de KasBox. Er vindt alleen VPN verkeer plaats op basis van het in de KasBox aanwezige certificaat. Omdat dit certificaat de publieke sleutel van de KAS BANK bevat kan er dus alleen met de KAS BANK verbonden worden.

Virussen, worms en trojan horses Er kan door de klant geen software op de KasBox worden geïnstalleerd: dit wordt niet toegestaan door het besturingssysteem. Daarnaast is de KasBox hardwarematig beveiligd: er is geen cdrom speler in de KasBox aanwezig en het gebruik van de beschikbare interfaces is uitgeschakeld waardoor er ook geen USB stick of externe harddisk aangesloten kan worden. Door de eerder genoemde firewall is het ook niet mogelijk om via het netwerk (dus ook het internet) toegang te krijgen tot de KasBox: alleen uitgaande verbindingen met de server van de KAS BANK zijn toegestaan.

Keyloggers Softwarematige keyloggers worden afgedekt door bovenstaande punt. Een hardwarematige keylogger, geïntegreerd in bijvoorbeeld een toetsenbord, is lastiger te voorkomen. Hiertoe zou de KasBox geleverd kunnen worden met een eigen toetsenbord waarvan het gebruik softwarematig wordt afgedwongen. Ook biometrische beveiliging is hier een goede oplossing.

Gebruik buiten het kantoor van de klant Er is door KAS BANK aangegeven dat alleen vanaf de locatie van de klant gebruik mag worden gemaakt van de KasBox. Hierbij dient aangemerkt te worden dat een technische oplossing waarmee dit gerealiseerd kan worden nagenoeg onmogelijk is. Dit geldt ook voor de andere voorstellen.

Om het te bemoeilijken kan bijvoorbeeld een check op IP adres of uitgaand telefoonnummer worden gedaan.

7.4.2 Uitrol

Klanten van de KAS BANK die online transacties willen doen ontvangen van de KAS BANK een KasBox, of in het geval van meerdere werkplekken meerdere KasBoxen. Eventueel kan er standaard een extra KasBox worden meegeleverd als backup. Daarbij wordt dan een N+1 principe aangehouden waarbij N staat voor het aantal benodigde KasBoxen. Mocht er een KasBox defect blijken te zijn dan is er een directe vervanging beschikbaar waarna het defecte exemplaar wordt geretourneerd en vervangen door een nieuwe.

7.4.3 Installatie

De KasBox kan door de gebruiker zelf geïnstalleerd worden. Na plaatsing sluit de gebruiker een monitor, toetsenbord en muis aan (eventueel via een KVM switch) alsmede de bijgeleverde smartcard-reader. Vervolgens wordt de KasBox aangesloten op het stroomnet, het netwerk en eventueel het telefoonnet.

De eerste keer dat de KasBox wordt aangezet verschijnt een eenvoudig configuratiemenu. In dit menu kan de gebruiker aangeven hoe hij wil verbinden met de KAS BANK: via het internet of via de telefoonlijn. Hij kan hiervoor zijn netwerkinstellingen configureren (of kiezen voor automatische configuratie middels DHCP) en een eventuele buitenlijn voor verbinden via de telefoon.

Met behulp van een troubleshooting optie kan de gebruiker zijn verbindingen testen (bijvoorbeeld ping en traceroute).

7.4.4 Onderhoud en updates

De KasBox vereist weinig tot geen onderhoud. Het bevat geen bewegende delen of onderdelen die aan slijtage onderhevig zijn. Updates worden automatisch geladen en geïnstalleerd op het moment dat de KasBox verbinding maakt met de KAS BANK. Hiervoor is geen actie van de gebruiker nodig en de gebruiker hoeft dit niet te merken. De KasBox zal na een update hoogstens herstarten.

In het geval van de noodzaak van een grote update die niet automatisch volgens bovenstaande methode kan worden uitgevoerd ontvangt de klant een geupdate KasBox van de KAS BANK, waarna de oude KasBox wordt geretourneerd.

7.4.5 Support

Als de KasBox is geïnstalleerd en verbinding heeft, is er weinig technische support nodig. Eenmaal verbonden kan de KasBox door de KAS BANK op afstand worden gemonitord, waarbij eventuele problemen kunnen worden gedetecteerd. Bij een defect wordt een backup exemplaar aangesloten of wordt een nieuwe toegezonden.

Functionele support in de vorm van gebruikersvragen zijn vooral afhankelijk van de gebruiksvriendelijkheid van de interface, de volledigheid en duidelijkheid van

de handleiding en de beschikbaarheid van online bronnen als *Frequently Asked Questions*. Dit is overigens evengoed het geval bij een softwareoplossing.

Supportvraag zal in principe alleen ontstaan bij de installatie waarbij netwerkproblemen de voornaamste oorzaak zijn. Daarbij zal een deel opgelost kunnen worden over de telefoon of per email, een (kleiner) deel zal bezoek van een monteur vereisen. Een (niet gefundeerde) schatting van deze aantallen is als volgt:

	Percentage
Geen support nodig	80%
Support per telefoon/email	15%
Monteur ter plaatse	5%

7.4.6 Flexibiliteit

De KasBox is standaard voorzien van een webbrowser voor het gebruik van KasWeb. Hiermee is het mogelijk gebruik te maken van andere webbased diensten zoals webmail. Mocht een toekomstige toepassing specifieke software vereisen dan kan deze software via de remote update mogelijkheid op de KasBox worden geïnstalleerd. Ook kan er gebruik worden gemaakt van een remote sessie applicatie zoals citrix of een virtual machine zoals VMware.

7.5 De KAS BANK omgeving

Binnen de KAS BANK hebben we een vijftal servers gedefiniëerd:

De KasWeb server: De feitelijke applicatieserver.

Het mainframe: Bevat onder andere de database met gegevens.

De Active Directory server : Voor gebruikerbeheer en authenticatie.

De VPN server (de F5) : Voor het accepteren van VPN verbindingen vanaf de KasBox.

Een reverse proxy : Voor het accepteren van SSL sessies vanaf het internet.

Deze servers worden respectievelijk in het interne netwerk (de eerste drie) en de DMZ (de laatste twee) geplaatst.

Gebruikers van de KasWeb service via internet, dus zonder de KasBox, maken gebruik van de reverse proxy. Hierbij wordt met deze reverse proxy een SSL sessie opgebouwd waarop deze server vervolgens met de KasWeb server communiceert. Dit heeft als doel loadbalancing (de reverse proxy server onderhoudt de verbindingen en kan bepaalde gegevens cachen) en veiligheid (de KasWeb server is niet direct vanaf het internet te bereiken).

Een verbinding vanaf de KasBox wordt opgezet met de F5 server. Over deze verbinding kan vervolgens een sessie worden opgebouwd naar de KasWeb server. Deze F5 is volgens de hoogste beveiligingsstandaarden ingericht en speciaal voor dit doeleinde geschikt.

De Active Directory server wordt door de andere servers aangesproken voor het authenticeren van de gebruikers en het controleren van certificaten.

Het mainframe bevat de database met de feitelijke gegevens die middels KasWeb worden ontsloten.

7.6 Procedures

Het is van belang procedures te definiëren met betrekking tot het gebruik van de KasBox en smartcards.

7.6.1 Verlies of diefstal van KasBox of smartcards

In het geval van verlies of diefstal van de KasBox of een smartcard dient dit direct gemeld te worden aan KAS BANK zodat de bijbehorende certificaten kunnen worden geblokkeerd.

7.6.2 Gebruik buiten het kantoor van de klant

Er is door KAS BANK aangegeven dat alleen vanaf de locatie van de klant gebruik mag worden gemaakt van de KasBox. Hiertoe kan een check op IP adres of uitgaand telefoonnummer worden gedaan. Indien er later besloten wordt toch gebruik buiten de eigen locatie toe te staan dan kan dit worden opgeheven en kan gekeken worden naar een draagbaardere versie van de KasBox.

7.6.3 Uitgifte van certificaten

Een certificaat is persoonlijk en mag slechts persoonlijk op vertoon van een geldige identificatie worden uitgegeven. De Nederlandse wetgeving laat echter ruimte om een certificaat uit te geven op basis van een alias en deze vervolgens te koppelen aan een persoon. Dit maakt het certificaat minder gevoelig voor mutaties door bijvoorbeeld verloop in het personeelsbestand van de klant.

8 Dreigingenanalyse

In de dreigingenanalyse noemen we een aantal mogelijke dreigingen en aanvallen met betrekking tot online communicatie en transacties. Een aantal hiervan zijn algemene dreigingen waar andere voorstellen ook mee te maken hebben, een aantal zijn specifiek voor onze oplossing.

8.1 Communicatie

8.1.1 Het niet beschikbaar zijn van een internetverbinding

Indien (tijdelijk) geen internetverbinding beschikbaar is kan gebruik worden gemaakt van de telefoonlijn. Hiervoor kan de KasBox worden aangesloten op het telefoonnet en kan ingebeld worden op een server van de KAS BANK. De functionaliteit is hierbij hetzelfde als een verbinding via het internet.

Risico continuïteit	laag
Risico veiligheid	laag

8.1.2 Denial of service

Met denial of service wordt bedoeld dat een kwaadwillende partij de client of de server overspoelt met dusdanig veel verkeer dat de internetverbinding “vol” raakt en er geen informatie meer uitgewisseld kan worden tussen de klant en de KAS BANK. Hiermee kan de kwaadwillende partij geen vertrouwelijke informatie bemachtigen maar hiermee wordt wel bereikt dat er geen inzage of transacties meer mogelijk zijn over het internet.

Het is nog steeds mogelijk om te communiceren met de KAS BANK via de telefoonlijn, zoals eerder uitgelegd.

Risico continuïteit	laag
Risico veiligheid	laag

8.1.3 Man in the middle

Bij een man-in-the-middle aanval doet een kwaadwillende partij zich aan beide partijen voor als de ander: aan de client als de server en aan de server als de client. Hierbij is het de bedoeling dat de beveiligde sessies worden opgebouwd met deze kwaadwillende partij waardoor deze inzicht heeft in het verkeer en eventueel informatie kan wijzigen.

Doordat gewerkt wordt met certificaten aan zowel de kant van de client als de kant van de server is het niet mogelijk een dergelijke aanval uit te voeren: de kwaadwillende partij heeft namelijk geen weet van de private sleutels en kan zich derhalve niet naar de beide partijen authenticeren als zijnde de andere partij. Zonder authenticatie wordt er geen beveiligde verbinding opgebouwd en kan er geen sessie worden gestart.

Risico continuïteit	laag
Risico veiligheid	laag

8.1.4 Session Hijacking

Session hijacking is het overnemen van een sessie door een derde, kwaadwillende, partij. Hiertoe breekt deze partij in op de sessie en doet alsof hij een van de deelnemende partijen is.

Omdat het een dubbel-versleutelde communicatie betreft (een versleutelde sessie vindt plaats over een versleutelde tunnel) en de derde partij niet op de hoogte is van de wederzijdse sleutels van zowel de verbinding als de sessie, is het niet mogelijk om de sessie op deze manier over te nemen.

Risico continuïteit	laag
Risico veiligheid	laag

8.1.5 Phising

Bij Phising doet een kwaadwillende partij zich voor als de bank om zo gegevens van de gebruiker te bemachtigen (zoals wachtwoorden).

Omdat in onze oplossing zowel de KasBox als een smartcard als een wachtwoord nodig zijn heeft een kwaadwillende niets aan een wachtwoord alleen. Toch bestaat het gevaar dat het achterhalen van wachtwoorden onderdeel is van een groter plan waarbij later een smartcard en bijbehorende KasBox worden gestolen. Hiervoor moet aan de gebruikers duidelijk worden gemaakt dat de KasBank nooit om een wachtwoord zal vragen. Met een biometrische authenticatie is er helemaal geen risico omdat de gebruiker geen wachtwoorden heeft om weg te geven.

Risico continuïteit	laag
Risico veiligheid	laag

8.2 KasBox & Smartcard

8.2.1 Diefstal van de KasBox

Indien slechts de KasBox gestolen wordt is er geen risico. Zonder smartcard kan er geen verbinding worden gemaakt met de KAS BANK en is het niet mogelijk om inzage of transacties te doen. Gebruik met een andere smartcard is niet mogelijk omdat de KasBox op de server van de KAS BANK gekoppeld is aan één of meerdere smartcards van de klant.

Als de diefstal aan de KAS BANK wordt gemeld kan de KasBox geblokkeerd worden in de database van de KAS BANK waardoor hij niet meer kan worden gebruikt. De klant ontvangt dan een nieuwe KasBox.

Risico continuïteit	medium
Risico veiligheid	laag

8.2.2 Diefstal van de smartcard

Indien slechts de smartcard wordt gestolen is er geen risico. Zonder KasBox kan er geen verbinding worden gemaakt met de KAS BANK en is het niet mogelijk om inzage of transacties te doen. Gebruik met een andere KasBox is niet mogelijk omdat de smartcard op de server van de KAS BANK gekoppeld is aan één of meerdere KasBoxen. Ook is er een wachtwoord of biometrische authenticatie nodig om de certificaten op de smartcard te ontsluiten.

Als de diefstal aan de KAS BANK wordt gemeld kan de smartcard geblokkeerd worden in de database van de KAS BANK waardoor hij niet meer kan worden gebruikt. De klant ontvangt dan een nieuwe smartcard.

Risico continuïteit	medium
Risico veiligheid	laag

8.2.3 Diefstal van de smartcard en de KasBox

Indien zowel de KasBox als de smartcard worden gestolen is er geen risico zolang de bijbehorende wachtwoorden niet bekend zijn of als er gebruik wordt gemaakt van biometrische authenticatie. Er kan welliswaar verbinding worden gemaakt met de KAS BANK maar het is niet mogelijk om inzage of transacties te doen.

Als de diefstal aan de KAS BANK wordt gemeld kunnen de smartcard en de KasBox geblokkeerd worden in de database van de KAS BANK waardoor ze niet meer kunnen worden gebruikt. De klant ontvangt dan een nieuwe smartcard en een nieuwe KasBox.

Risico continuïteit	medium
Risico veiligheid	laag

8.2.4 Diefstal van de smartcard, de KasBox en de bijbehorende wachtwoorden

Indien zowel de KasBox als een smartcard als de bijbehorende wachtwoorden worden gestolen, is er een groot veiligheidsrisico. Met deze combinatie heeft een kwaadwillende alle middelen in handen om zich voor te doen als de gebruiker en gebruik te maken van inzage en transactiediensten.

Tijdige melding van de diefstal aan de KasBank kan de risico's beperken doordat de KasBank de smartcard en KasBox kan blokkeren in de database. Ook kan het risico beperkt worden door een check op IPadres en/of telefoonnummer te doen voordat een verbinding wordt geaccepteerd. Biometrische authenticatie biedt de beste bescherming. Er moet daarbij wel worden gedacht aan de veiligheid van de klant: deze kan met lichamelijk geweld worden gedwongen transacties uit voeren.

Risico continuïteit	medium
Risico veiligheid	hoog

8.2.5 Openen van de KasBox

In de KasBox is een certificaat opgeslagen. Een kwaadwillende zou de KasBox kunnen openen met het doel dit certificaat uit te lezen. Het uitlezen van het certificaat is op zichzelf geen risico. Het bevat geen vertrouwelijke informatie en het nut ervan is buiten de KasBox zeer gering:

- Met het certificaat alleen kan geen verbinding worden opgebouwd.
- Met het certificaat alleen kan eerdere communicatie niet worden ontsleuteld.
- Met het certificaat kunnen geen inzage en transacties worden gedaan.

Het openen van de KasBox heeft voor de klant geen toegevoegde waarde. Daarmee wordt de verzegeling van de KasBox verbroken waardoor de klant het recht op support verliest. Het openen van de KasBox door een kwaadwillende heeft, door het beperkte nut van het certificaat, ook geen toegevoegde waarde. Daarnaast gelden dezelfde punten als bij diefstal van de KasBox (wat in principe voorafgaat aan het openen). Mocht een kwaadwillende de KasBox toch openen dan is het certificaat niet uit te lezen zonder geldige smartcard omdat het versleuteld is opgeslagen.

Risico continuïteit	laag
Risico veiligheid	laag

8.2.6 Diefstal van de private sleutel van de KAS BANK

In het onwaarschijnlijke geval dat de private sleutel van de KAS BANK in verkeerde handen valt is er enig risico. De kwaadwillende partij kan zich naar de klant voordoen als de KAS BANK maar, omdat hij geen weet heeft van de publieke sleutels van de klant, zal de handshake mislukken. Mocht de sleutel in handen vallen van een partij die klant is bij de KAS BANK en derhalve een KasBox en smartcard heeft dan is het mogelijk dat deze klant transacties vervalst en signeert met de sleutel van de KAS BANK.

Mocht de sleutel van de KAS BANK gecompromitteerd raken dan is het nodig dat alle KasBoxen en alle smartcards worden vervangen door exemplaren met de nieuwe publieke sleutel. Hierdoor is het een groot risico voor de continuïteit.

Risico continuïteit	hoog
Risico veiligheid	medium

9 Realisatie

Voordat de KasBox realiteit kan worden moet er nog verder onderzoek worden gedaan en moeten procedures worden gedefiniëerd. De KasWeb omgeving en de KasBox moeten worden ingericht en geconfigureerd en specifieke software moet worden geschreven. Hiervoor dient een KasBox projectgroep te worden opgericht. Hierbij kan eventueel gebruik worden gemaakt van HBO of universitaire stagiaires.

Aan de klanten die terughoudend zijn over het plaatsen van een black box in hun netwerk moet zekerheid worden verschaft over de veiligheid ervan. Hiervoor zou de KasBox voorzien kunnen worden van een externe certificering.

We zijn in dit document uitgegaan van smartcards in combinatie met wachtwoorden omdat er twijfel bestond over de huidige stand van techniek met betrekking tot biometrische identificatie: deze zou nog onvoldoende ver zijn om ontsluiting van een smartcard te faciliteren. Wij hebben dit onderzocht en het blijkt dat dit inmiddels goed mogelijk is. Daarom zou dit zeker meegenomen kunnen worden.

9.1 Planning

Uitgaande van een projectgroep van 5 man denken wij dat een werkende KasBox infrastructuur binnen een half jaar mogelijk moet zijn. Hierbij speelt mee dat de KasBox op afstand is te updaten waardoor de ontwikkeling nog door kan gaan na implementatie.

9.2 Kosten

Om ons voorstel verder te onderzoeken zijn er twee mogelijkheden. De eerste mogelijkheid is om één of meerdere stagiaires dit verder te laten uitwerken. Dit zal minder snel tot resultaat leiden, maar zal behoorlijk in de kosten schelen. De tweede mogelijkheid is in-house. Hiervoor zal een projectgroep dit voorstel verder uitwerken. Hiermee zal naar alle waarschijnlijkheid een sneller resultaat behaald worden. Dit heeft de kosten als nadeel, aangezien de werknemers duurder zijn dan stagiaires.

Stel dat een keuze wordt gemaakt om dit voorstel in-house uit te werken, dan zijn de kosten afhankelijk van het aantal personen dat wordt ingezet op het project. In deze berekening wordt uit gegaan van 5 personen over een periode van 6 maanden. Er dient opgemerkt te worden dat dit onderzoek eenmalig is.

personen	periode	kosten pp	totaal
5	6 maanden	5000 euro	150.000 euro

Doordat we in onze oplossing gebruik maken van open software hoeven we geen extra licenties te betalen. De enige kosten die hiervoor verder gelden is de hardware.

KasBox	250 euro
Smartcard-reader	100 euro
Smartcards	10 euro

Wanneer we de KasBox uitrollen in de situatie zoals die nu is en rekening houden met één standby box per klant dan zien de kosten er als volgt uit: In onderstaande tabel is te zien hoeveel het kost om 500 KasBoxen uit te rollen met een totaal van 150 KasBoxen standby. Tevens zijn voor het totaalbeeld de kosten voor het personeel meegenomen.

	aantal	kosten (euro's)	kosten totaal (euro's)
Werkplekken	500	350	175.000
Standby	150	350	52.500
Personeel	5	30.000	150.000
Totaal met personeelskosten			377.500
Totaal zonder personeelskosten			227.500

In de schema's worden geen bedragen gewijd aan smartcards. Afhankelijk van het aantal wat hiervan afgenomen wordt kunnen de prijzen behoorlijk verschillen. Tevens is het lastig om hier nu al een uitspraak over te doen. Een nieuwe omgeving kan tevens opschoning betekenen. Ook de kosten van de uitrol worden in het vorige schema niet meegenomen.

Voor het half jaar na het onderzoek en de implementatie wordt de projectgroep ingezet om problemen/uitdagingen snel en goed op te lossen. Wanneer dit goed georganiseerd wordt, worden de kosten in de komende jaren minder. De projectgroep van 5 personen voor 6 maanden kost 150.000 euro. Als er vanuit gegaan wordt dat het merendeel van de problemen/uitdagingen is opgelost kunnen er minder fte in het project gepland worden. We gaan uit van 2 fte in het tweede jaar en in het derde jaar gaan we ervan uit dat 1 tot 1.5 fte afdoende is. Wat in totaal 210.000 euro is als we uitgaan van 1.5 fte in het derde jaar. In totaal wordt dit voor een schatting voor 3 jaar: 737.500 euro inclusief personeelskosten.

	Kosten (euro)
Jaar 1	377.500
Jaar 2	120.000
Jaar 3	90.000
Totaal over 3 jaar	737.500

9.2.1 Andere voorstellen

Hieronder is een tabel te zien waarin wordt aangegeven wat de kosen zijn voor de andere voorstellen. Hier wordt net als in onze berekening uitgegaan van 150 klanten en 1500 gebruikers.

	Kosten 3 jaar	Percentage eenmalig	Percentage variabel
SWIFT	4 miljoen	?	?
Partij U	900.000	30%	70%
Partij R	900.000	50%	50%
Partij A	1.000.000	70%	30%

10 Conclusies en aanbevelingen

In dit deel geven we onze conclusies en hierna volgen onze aanbevelingen.

10.1 Conclusies

- PKI vormt een goede basis voor de beveiliging, mits een sterke authenticatie wordt gebruikt.
- Een softwarematige oplossing waarbij geen controle bestaat over de omgeving van de klant laat risico's open.
- Onze oplossing
  - neemt een groot deel van de risico's van de softwareoplossing weg.
  - biedt een standaard infrastructuur die in de toekomst ook voor andere doeleinden gebruikt kan worden.
  - is gebruikers- en beheerdersvriendelijk. Daarnaast vergt het weinig tot geen onderhoud.
  - gebruikt de F5 waardoor geen nieuwe server(s) aangeschaft hoeft te worden.
  - concureert qua prijs met de andere voorstellen.
  - is haalbaar (eventueel na uitwerken met een bredere scope)

10.2 Aanbevelingen

We bevelen aan verder onderzoek te doen naar de KasBox. Dit kan eventueel in het kader van een afstudeerstage of researchproject gedaan worden. In eerste instantie kan de KasBox geleidelijk uitgerold worden onder klanten die zeer grote transacties doen, terwijl klanten die slechts inzagefunctionaliteit of kleine transacties wensen (voorlopig) van de huidige infrastructuur gebruik blijven maken. Eventueel kan er nog een tussenliggend beveiligingsniveau worden gedefiniëerd waarin minder grote transacties met behulp van een PKI oplossing zonder KasBox gedaan kunnen worden. Hierdoor is het mogelijk om vanaf willekeurige locaties kleine transacties toe te staan.

11 Discussie

De andere partijen hebben, op SWIFT na, allemaal een oplossing gepresenteerd conform de wensen van de KAS BANK met software bij de klant. Hierbij moet in gedachten worden gehouden dat het commerciële partijen zijn die proberen een opdracht binnen te slepen. KAS BANK heeft aangegeven een oplossing zonder hardware te prefereren dus dat wordt gerespecteerd door de opdrachtnemers.

Omdat wij geen commerciële belangen hebben, hebben we vanuit een ander perspectief naar het probleem kunnen kijken. We werden minder beperkt door specifieke eisen en hebben vanuit het oogpunt van veiligheid een oplossing bedacht.

Referenties

[1] *Kasbank website*
http://www.kasbank.nl

[2] *Network Security, private communication in a public world*
ISBN 0-13-046019-2

[3] *Firepass reference sheets*

[4] *Google is your friend*
http://www.google.nl

[5] *Whatis.com*
http://www.whatis.com

[6] *USB Smartcardreader*
http://www.saflink.com/partners/device_pages/67101-00000.htm

A KasBox: techniek

Het principe is een eenvoudige computer zonder bewegende delen met een stripped down Linux kernel.

A.1 Hardware

- VIA epia bord met onboard VGA, netwerkkaart, CF reader
- Behuizing met voeding
- 128mb CF card (als harddisk)
- 56k6 modem

De KasBox bevat de volgende aansluitingen:

- Netvoeding
- Monitor
- Toetsenbord
- Netwerk
- Telefoon
- smartcard-reader (USB)

Verder kan voor het gebruik van de smartcards een USB smartcardreader met fingerprintreader worden meegeleverd.

A.2 Software

Het OS van de KasBox is een stripped down Linux. Hierop draait een minimale X server met een browser, bijvoorbeeld Mozilla FireFox. Voor het opzetten van een VPN verbinding wordt gebruik gemaakt van stunnel in combinatie met OpenSSL.

Voor toekomstige applicaties kan er gekozen worden voor het gebruik van een virtual machine of een remote session client als Citrix.

- Minimale Linux install
- X-Server met browser (Mozilla FireFox)
- Stunnel en OpenSSL
- (X-server of Citrix)

B Overzicht

Op de volgende pagina is een overzicht te zien van de de oplossingen van de verschillende partijen.

	EU Richtlijn	SWIFT	Partij U	Partij R	KasBox
Klantomgeving	Verantwoordelijkheid klant.	Verantwoordelijkheid klant.	Verantwoordelijkheid klant.	Verantwoordelijkheid klant.	KasBox van KAS BANK
Netwerkverbinding	'Veilig'(Aanbieder is verantwoordelijk voor de technische invulling.)	VPN-verbindingen over eigen netwerk-infrastructuur	VPN-verbindingen over internet.	VPN-verbindingen over internet.	VPN-verbindingen over internet of telefoonlijn
PKI, Trust Third Party	TTP garandeert geldigheid certificaten (= elektronische identiteit en handtekening).	SWIFT is TTP voor KAS BANK en client.	Partij U is TTP voor KAS BANK en client.	KAS gebruikt geen TTP.	KAS gebruikt geen TTP (buiten scope)
PKI, Gepersonaliseerde certificaten	Voorgeschreven.	Mogelijk, niet toegepast door KAS	Mogelijk, niet toegepast voor KAS	Mogelijk, niet toegepast voor KAS	Mogelijk (buiten scope)
PKI, Certificaten uitgereikt na identificatie m.b.v. paspoort	Voorgeschreven.	Alleen Security Officer(s) bij de klant worden geïdentificeerd m.b.v. paspoort.	Inrichting te bepalen door aanbieder.	Inrichting te bepalen door aanbieder.	Inrichting te bepalen door aanbieder (buiten scope).
PKI, Private sleutel.	Private sleutel uitsluitend bij eigenaar bekend.	Private sleutel uitsluitend bij eigenaar bekend.	Private sleutel uitsluitend bij eigenaar bekend.	KAS genereert en kent private sleutels client.	Private sleutel uitsluitend bij eigenaar bekend.
Koppeling gebruiker / certificaat.	In opzet moet één certificaat één gebruiker identificeren.	Certificaat ontsloten met PIN-code.	Certificaat ontsloten met PIN-code.	Certificaat biometrisch ontsloten (of PIN-code).	Certificaat biometrisch ontsloten (of PIN-code).
Beveiliging certificaat	'Veilig' (Aanbieder is verantwoordelijk voor de technische invulling.)	Certificaat opgeslagen in smartcard.	Certificaat opgeslagen in smartcard.	Certificaat opgeslagen in smartcard.	Certificaat opgeslagen in smartcard en in de KasBox.
Locatie	niet bepaald	Uitsluitend vooraf bepaald klant-adres (bedrijf).	Elke pc ter wereld. Controle op juiste locatie mogelijk.	Elke pc ter wereld. Controle op juiste locatie mogelijk.	KasBox. Controle op juiste locatie mogelijk.
Verbinding afhankelijk van aanwezigheid certificaat.	niet bepaald	Verbinding afhankelijk van aanwezigheid smartcard.	Verbinding afhankelijk van aanwezigheid smartcard.	Verbinding afhankelijk van aanwezigheid smartcard.	Verbinding afhankelijk van aanwezigheid smartcard.