

0101UZI0100REGISTER10111

Toelichting op SDK

Uitgave : agentschap CIBG
Versie : 1.0
Datum : 6-2-2008
Bestandsnaam : 20080206 - Toelichting SDK op V1.0.doc

Inhoudsopgave

1. Inleiding	3
1.1 Wat is de SDK kit?	3
1.2 Voor wie is de SDK bedoeld?	3
1.3 Waarvoor kan de SDK gebruikt worden?	3
1.4 Hoe kan ik aan de SDK komen?	3
1.5 E-mailen van bestand	3
1.6 Geen support op inhoud van SDK kit	3
1.7 Wat bevat de SDK niet?	3
2. Inhoud van de SDK	4
2.1 Data Sheets	4
2.2 Weblinks	5
2.3 Presentation	5
2.4 Specifications	5
2.5 Samples	6

Versiehistorie

Versie	Datum	Status	Change	Toevoegingen en wijzigingen	Hst/§
0.1	4-6-2008	concept		1° opzet	Geheel
0.2	5-6-2008	concept		Aanpassingen na 1 ^e review & Tekstuele aanpassingen voor website	Geheel
1.0	6-6-2008	Definitief			Geheel

1. Inleiding

1.1 Wat is de SDK kit?

SDK staat voor Software Development Kit. Het betreft een verzameling handleidingen en voorbeeldcodes. Deze SDK bevat documentatie en programmeertalen voorbeeldcodes in C++ 6 en C++ dot.Net (2003). C++ en dot.net zijn. Daarnaast zijn er een aantal links genoemd naar handige startpunten voor de ontwikkeling van applicaties met de UZI-pas.

1.2 Voor wie is de SDK bedoeld?

De SDK wordt gebruikt door softwareontwikkelaars en andere afnemers van testpassen

1.3 Waarvoor kan de SDK gebruikt worden?

De softwareontwikkelaar is bezig om een applicatie geschikt te maken voor gebruik van de UZI-pas. Om dit te bewerkstelligen moeten bepaalde programmacodes worden ingevoerd in de applicatie.

1.4 Hoe kan ik aan de SDK komen?

De SDK kit is beschikbaar op de website, maar kan op verzoek een toegezonden worden

1.5 E-mailen van bestand

Het kan voorkomen dat het MSI bestand door de mailserver van de klant wordt tegengehouden. Mocht dit gebeuren dan kan de ingepakte ZIP versie worden gemaïld.

1.6 Geen support op inhoud van SDK kit

Er wordt geen inhoudelijke support gegeven op de SDK. Ervaring heeft geleerd dat programmeurs hiermee uit de voeten kunnen. Wel staat beschreven wat er allemaal in de SDK zit en waar kan ik wat terugvinden.

1.7 Wat bevat de SDK niet?

De SDK bevat geen handleidingen hoe bepaalde zaken ingesteld moeten worden (voorbeeld: Terminal services, Citrix, aanmaken PKCS#10). Deze kunnen op verzoek van de klant apart toegezonden worden.

2. Inhoud van de SDK

2.1 Data Sheets

Dit zijn documenten waarin in het kort beschreven staat welke functionaliteit er met de Middleware te gebruiken is. Deze informatie is per categorie beschreven. Het betreft geen handleidingen hoe dit te realiseren.

De laatste versies van de documentatie is terug te vinden op website van het UZI-register

SafeSign_Datasheet_Check Point.pdf

Toelichting over het gebruik van de AET Safesign software onder Check Point VPN

SafeSign_Datasheet_Citrix.pdf

Toelichting over het gebruik van de AET Safesign software onder Citrix

SafeSign_Datasheet_Microsoft-VPN.pdf

Toelichting over het gebruik van de AET Safesign software onder Microsoft VPN

SafeSign_Datasheet_NCP-VPN.pdf

Toelichting over het gebruik van de AET Safesign software onder NCP VPN

SafeSign_Datasheet_Terminal-Server.pdf

Toelichting over het gebruik van de AET Safesign software onder Terminal Server

SafeSign_Datasheet_WinCE-PocketPC.pdf

Toelichting over het gebruik van de AET Safesign software onder Windows CE / PocketPC

SafeSign_Datasheet_Windows-Logon.pdf

Toelichting over het gebruik van de AET Safesign software in combinatie met Windows Smart Card logon

SafeSign_Datasheet_WLAN.pdf

Toelichting over het gebruik van de AET Safesign software in combinatie met een draadloos network.

SafeSign_Flyer_082005.pdf

Algemene informatie over de Safesign Middleware

White_Paper_SafeSign_v1.1.pdf

Uitgebreide informatie over de Safesign Middleware. Hierin staat onder andere de werking uitgelegd

2.2 Weblinks

Dit zijn links naar websites waar naslag te vinden is. Deze informatie is voor een ontwikkelaar handig om bij de hand te hebben. Hierin staat bijvoorbeeld beschreven hoe het PKCS verhaal in elkaar zit.

starting_points.html

Bevat een aantal links naar internetpagina's met daarop de volgende informatie:

Standards

<http://www.rsa.com/rsalabs/node.asp?id=2124>

Toelichting over RSA en PKCS#11

<http://www.rfc-ref.org/index.html>

Algemene website voor het opzoeken van RFC's

<http://www.iso.org/iso/home.htm>

Algemene website voor ISO normeringen / standaarden

Programming

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncapi/html/msdn_cryptapi.asp

Toelichting over de Microsoft Crypto API instructie

<http://jce.iaik.tugraz.at/products/index.html>

Link werkt niet meer. Is nu:

<http://jce.iaik.tugraz.at/sic/products>

Diverse crypto toolkits waaronder een SSL library voor ontwikkeling van een SSL/TLS client.

<http://java.sun.com/j2se/1.5.0/docs/guide/security/p11guide.html>

PKCS#11 in combinatie met Java.

Toolkit

<http://www.openssl.org/>

Op de bovenstaande pagina kan de tool OpenSSL worden gedownload

<http://www.entrust.com/products/list.htm>

Op de bovenstaande pagina kunnen hulpmiddelen van Entrust worden gedownload.

<http://www.eldos.com/>

Hier is SecureBlackBox tool te downloaden.

2.3 Presentation

SafeSign-software-development.pdf

In deze presentatie staat de techniek achter de UZI-pas toegelicht. Een goed startpunt.

2.4 Specifications

pkcs-11v2-11r1.pdf

In dit PDF bestand staat de gehele specificatie beschreven van PKCS#10. Voor C++ staan hierin de functies beschreven: Welke functies er zijn en wat de functies precies doen.

2.5 Samples

C++ 6 & C++ dot.net (2003)

Voor beide veel voorkomende programmeertalen heeft AET voorbeeldcodes beschikbaar gesteld. Dit zijn stukjes code die een programmeur kan gebruiken of inzien om zijn applicatie geschikt te kunnen maken voor gebruik van de UZI-pas.

Er zijn voor de volgende onderwerpen voorbeeldcodes beschikbaar: Authenticatie & Encryptie en maken gebruik van de PKCS#11 API.

Als een klant gebruikt maakt van een andere programmeertaal (vb: Delphi, Pascal, Java) kan met behulp van de geleverde voorbeeldcodes een vertaalslag worden gemaakt naar de andere taal.
