Vad är e-legitimation?

En e-legitimation kan jämföras med en vanlig id-handling, till exempel id-kort eller körkort. Med en e-legitimation kan du på ett säkert sätt legitimera dig på internet, till exempel vid godkännande och inlämnande av skattedeklaration över internet. Exempel på svenska myndigheter som accepterar e-legitimation är Skatteverket, Arbetsförmedlingen, Försäkringskassan och Centrala studiestödsnämnden.

Vad är Svensk e-legitimation?

Svensk e-legitimation är ett samarbete kring elektronisk identifiering och underskrift mellan tillhandahållare av e-tjänst i offentlig sektor (exempelvis myndigheter) och leverantörer av eID-tjänst, där leverantörerna på ett säkert sätt kan leverera standardiserade identitetsintyg till offentlig sektors e-tjänster.

E-legitimationsnämnden är central aktör och administrerar Svensk e-legitimation med stöd av tjänsteleverantören Cybercom Group AB.

Svensk e-legitimation är tänkt att vara i drift hos organisationer i offentlig sektor med e-tjänster senast halvårsskiftet 2016.

Finns det liknande lösningar i andra länder?

Ett antal länder i Europa har olika lösningar som baseras på samma standard som används i Svensk e-legitimation, standarden SAML.

Ved menas med LoA

LoA är en förkortning a Level of Assurance, motsvarande begrepp på svenska är tillitsnivå.

Vad menas med tillitsnivå

Regelverket för Svensk e-legitimation baseras på ett tillitsramverk som i sin tur bygger på ISO 29115 ”Information technology — Security techniques — Entity authentication assurance framework”.

I detta standardiserade ramverk definieras tillitsnivåerna 1 till 4 där högre siffra innebär större tillit till systemet. Nivå 1 motsvarar den vanliga typen av inloggning som används till publika webbtjänster som forum, företagshemsidor och liknande, ofta med användarnamn och lösenord. Denna nivå garanterar inte användarens identitet och ingår därför inte i det svenska tillitsramverket. Från nivå 2 och uppåt finns en ökande grad av tilltro till kontrollen av användarens identitet, den e-tjänst som använder e-legitimationstjänsten för identifiering av användarna kan med andra ord i allt högre utsträckning vara säker på att det är rätt användare som man kommunicerar med. Dessa högre nivåer behöver nyttja någon typ av legitimationslösning – det räcker inte med bara användarnamn och lösenord.

Vad är en kryptoalgoritm

En kryptoalgoritm är en matematisk procedur som används vid kryptering. Kryptering kan användas för att skydda information mot läsning eller förändring, den kan även användas för att bevisa vem det är som sänt information.

Vad är SAML

SAML är en förkortning av Security Assertion Markup Language, vilket är ett öppet dataformat för att utbyta information för legitimeringssyften. Svensk e-legitimation baseras på SAML version 2.0.

Vad är central infrastruktur

Med central infrastruktur avses Metadatatjänst och Anvisningstjänst, se nedan förklaringar av respektive begrepp

Vad är Anvisningstjänst

En Anvisningstjänst, eller Discovery Service, har som sitt syfte att avlasta de enskilda e-tjänsterna från att själva implementera stöd för hur användare väljer legitimeringstjänst för autentisering. Genom att en Anvisningstjänst finns tillgänglig kan e-tjänster styra sina användare dit för val av legitimeringsmetod (eller legitimeringstjänst). Anvisningstjänsten interagerar med användaren som gör sitt val och användaren, tillsammans med dennes val, styrs tillbaka till e-tjänsten som nu vet till vilken legitimeringstjänst användaren ska skickas för legitimering

Vad är COTS

COTS står för Commercial of the Shelf, dvs. i detta fall avses färdiga mjukvaruprodukter som går att köpa i stället för att utveckla dem själv.

Vad är Metadatatjänsten

En SAML federation som Svensk e-legitimation kan tillhandahålla information om deltagare genom så kallade metadata. Det kan exempelvis handla om information om andra deltagares tjänster, inklusive de uppgifter som krävs för ett säkert informationsutbyte mellan deltagarna. Det sistnämnda torde vara viktigaste användningsområdet för Metadata, att tillhandahålla de nycklar som krävs för säker kommunikation och informationsutväxling mellan tjänster.

Genom metadatatjänsten kan deltagare inhämta information om varandra. Som deltagare räknas såväl aktörer som levererar tjänster (Legitimeringstjänster, Attributstjänster, mm), som aktörer som konsumerar dessa tjänster (ex. e-tjänster som konsumerar tjänsten legitimering).

Metadata utgör en viktig gemensam informationsbas genom vilken deltagande aktörer kan erhålla viktig information.

Vad är best practices inom informationssäkerhetsområdet

Best practices är sammanställda regler och rekommendationer för hur man på ett lämpligt sätt bedriver utvecklingsarbete. Exempel på dessa är "Fundamental Practices for Secure Software Development" och “OWASP Testing Guide / Developer Guide”.

Vad är DoS/DDoS

DoS eller DDoS är en typ av belastningsattack. En DoS-attack kan bestå av något så enkelt som endast ett specialformaterat paket som orsakar att systemet kraschar eller tjänster slutar att fungera, den kan också överbelasta ett system med onormalt mycket trafik från ett annat (kraftfullare) system. Den första typen av attacker är ofta riktad mot en specifik tjänst som i många fall innehåller en sårbarhet eller är felaktigt konfigurerad.

DDoS är distribuerade attacker som vanligen bygger på angrepp genom att använda flera olika system för attacken. DDoS kan fungera oberoende av sårbarheter i det system som attackeras.

Vilken roll har MSB inom informationssäkerhetsområdet

MSB:s uppdrag inom informationssäkerhetsområdet är bl.a. att:

- stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området
- lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer
- rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället

MSB har även föreskriftsrätt inom informationssäkerhetsområdet samt ger även stöd när det gäller att förebygga och hantera it-incidenter.

Länktips

E.legitimation.se:
http://www.e-legitimation.se/

Mina vårdkontakter:

https://www.minavardkontakter.se/C125755F00329208/p/KONT-8ZSGV8?opendocument

Skatteverket:
https://www.skatteverket.se/privat/sjalvservice/allaetjanster/omelegitimation.4.18e1b10334ebe8bc80004811.html#