SSEK version 2.0

Säkra webbtjänster för affärskritisk kommunikation

Uppdatering av transportsäkerhet

2024-08-30

Gustaf Nyman, Apitek Aktiebolag

Sammanfattning

SSEK 2.0 specificerar hur säkra tjänster för informationsutbyte mellan organisationer utformas och bygger på ett antal vedertagna standarder för tjänster över Internet. Sedan 2006-05-10, då SSEK 2.0 utgavs, har dessa standarder utvecklats och SSEK bör utvecklas tillsammans med dem.

Detta dokument uppdaterar SSEK 2.0 punkt 5, speciellt 5.1 Transportsäkerhet. I övrigt gäller SSEK 2.0.

5 Säkerhet

Avseende säkerhet vid kommunikation över Internet har följande affärsbehov identifierats:

- Att information skyddas mot att bli läst eller manipulerad av obehöriga.
- Att information säkert kan härledas till avsändaren.

För att möta affärsbehoven avseende säkerhet uppfyller SSEK de säkerhetsaspekter som följande tabell beskriver. För detta ändamål använder SSEK säkerhetsmodellen PKI (Public Key Infrastructure) [PKI].

Aspekt	**Förklaring**	**Stöd i SSEK**
Sekretess	Meddelanden kan under transport inte läsas av andra än mottagaren.	TLS
Autentisering av mottagare	Mottagarens identitet är styrkt för avsändaren.	TLS med servercertifikat
Autentisering av avsändaren	Avsändarens identitet är styrkt för mottagaren.	TLS med (klient) organisationscertifikat
Integritet, riktighet	Meddelanden har inte förändrats under transport från avsändare till mottagare.	Signering med stämpelcertifikat
Oavvislighet	Avsändaren kan inte förneka att innehållet i ett meddelande skapats av dem.	Signering med stämpelcertifikat

SSEK delar upp säkerhetsaspekterna i transportsäkerhet (TransportLevelSecurity) och meddelandesäkerhet (MessageLevelSecurity).

5.1 Transportsäkerhet

SSEK specificerar två nivåer av transportsäkerhet:

- Sekretess och autentisering av mottagaren med TLS (SSL)
- Sekretess och autentisering av avsändare och mottagare med TLS (SSLWithClientCertificate)

SSEK kräver att minst transportsäkerhetsnivån SSL används. Transportsäkerhetsnivån SSL innebär att informationen skyddas mot att obehöriga kan läsa den samt att mottagaren är identifierad. Transportsäkerhetsnivån SSLWithClientCertificate innebär att även avsändaren identifieras. Det kan exempelvis användas vid publicering av tjänst som behöver skyddas mot åtkomst av obehöriga.

S001 TLS med serverautentisering (SSL) med lägsta version 1.2 [TLS1.2] SKALL användas.

S002 TLS med klientautentisering (SSLWithClientCertificate) KAN användas.

S003 En tjänsts transportsäkerhetsnivån SKALL anges i dess policy.

S009 TLS version 1.3 [TLS1.3] BÖR användas.

9 Referenser

[TLS1.2] RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2, https://datatracker.ietf.org/doc/html/rfc5246

[TLS1.3] RFC8446: The Transport Layer Security (TLS) Protocol Version 1.3, https://datatracker.ietf.org/doc/html/rfc8446