UPPSALA UNIVERSITET

Dnr UFV 2014/389

Riktlinjer för informationssäkerhet

Säkrare elektronisk kommunikation

- Tvåfaktorautentisering
- Kryptering och signering av e-post
- Elektronisk signering av dokument

Fastställda av: Säkerhetschef 2014-03-09

Reviderade: 2015-02-06

Innehållsförteckning

1 Inledning

Säkrare elektronisk kommunikation definieras i detta dokument som användning av en eller flera av nedanstående tjänster vid kommunikation av känslig information över nätet, t.ex. via e-post

- Tvåfaktorautentisering
- Kryptering och signering av e-post
- Elektronisk signering av dokument

2 Syfte

Att elektronisk kommunikation av känslig information vid universitetet sker enligt gällande lagar och förordningar.

Att ge stöd till universitetets verksamheter som har behov av förhöjd inloggningssäkerhet till informationssystem och IT-tjänster som hanterar känslig information med avseende på sekretess, riktighet och tillgänglighet.

Att elektronisk signering av dokument även ska bidra till effektivisering av dokumentflöden inom universitetet genom att reducera behovet av att skriva ut, faxa eller skicka med vanlig post.

3 Mål

Att alla informationssystem och IT-tjänster som hanterar känslig information med höga krav på sekretess, riktighet eller tillgänglighet, ska

- Införa tvåfaktorautentisering vid inloggning till systemet/tjänsten enligt *avsnitt 5.1* i dessa riktlinjer

Att känsliga personuppgifter enligt *13 § personuppgiftslagen (PUL)* och annan för universitetet känslig information som kommuniceras via e-post, ska

- Krypteras enligt *avsnitt 5.2* i dessa riktlinjer

Att elektroniska dokument av karaktären avtal, beslutsprotokoll eller som innehåller känslig information och där motsvarande pappersdokument skulle ha undertecknats med en handskriven namnteckning, ska

- Signeras elektroniskt enligt *avsnitt 5.3* i dessa riktlinjer för att skydda ett dokuments integritet och autenticitet (äkthet)

Att även andra typer av dokument som idag skrivs ut, undertecknas för hand och faxas eller skickas med post istället använder elektronisk signering för att effektivisera interna och externa dokumentflöden med avseende på tid och kostnad.

4 Omfattning

4.1 Tvåfaktorautentisering

Vissa informationssystem och IT-miljöer inom universitetet lagrar och hanterar information med höga eller särskild höga krav på skyddsåtgärder med avseende på sekretess, riktighet eller tillgänglighet, t.ex. forskningsdata, skyddade identiteter och andra känsliga personuppgifter.

För att säkerställa att endast behöriga personer har åtkomst till sådan information bör s.k. stark autentisering användas. Detta innebär att en användare vid inloggning måste identifiera sig med två faktorer; något man vet och något man har (t.ex. en säkerhetsdosa eller ett s.k. smart kort). Beroende på jurisdiktioner (sakområden) finns det dock olika krav, eller tillitsnivåer, på den andra faktorn.

4.2 Kryptering och signering av e-post

4.2.1 Inledning

Kryptering av e-post är en process där man använder mottagarens certifikat för att kryptera innehållet i ett brev på ett sådant sätt att endast personer med tillgång till mottagarens certifikat kan läsa innehållet i klartext. *Signering* av e-post verifierar för mottagaren att brevets innehåll inte har förändrats mellan avsändande och mottagande. En elektronisk signatur, eller underskrift, identifierar, precis som en vanlig handskriven underskrift, personen som skickar e-post.

4.2.2 Kryptering av känsliga personuppgifter

Personuppgiftslagen (PUL)
Uppsala universitet har enligt personuppgiftslagen (1998:204) en skyldighet att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas vid myndigheten. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, och
- hur känsliga de behandlade personuppgifterna är

Definitioner
Med känsliga personuppgifter avses enligt *13 § personuppgiftslagen (1998:204):*

Personuppgifter som avslöjar
- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse, eller
- medlemskap i fackförening, samt

Personuppgifter som rör hälsa eller sexualliv

Med sekretesskyddade uppgifter avses uppgifter som omfattas av sekretess enligt bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Särskilda bestämmelser om behandling av personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden finns i *21 § personuppgiftslagen.*

När ska kryptering ske
E-postmeddelanden ska krypteras när informationen innehåller känsliga personuppgifter, sekretesskyddade uppgifter eller personuppgifter om lagöverträdelser m.m. enligt 21 § personuppgiftslagen enligt Definitioner ovan.

Vem är skyldig att kryptera e-post med känsliga personuppgifter
Alla medarbetare och övriga verksamma vid Uppsala universitet.

Hur ska krypteringen ske
Se *avsnitt 5.2*.

4.2.3 Kryptering av annan känslig information

Enligt universitetets *Riktlinjer för lösenordshantering (UFV 2013/1490)* ska lösenord aldrig kommuniceras via e-post. Det kan även finnas goda skäl att överväga att kryptera e-post som innehåller känslig forskningsinformation, tentamensuppgifter, inköps- och upphandlingsinformation etc.

4.3 Elektronisk signering av dokument

En elektronisk signatur, eller underskrift, identifierar, precis som en vanlig handskriven underskrift, personen som undertecknar ett dokument. En elektronisk underskrift svår att förfalska, eftersom den innehåller krypterad information som är unik för undertecknaren. Den kan lätt verifieras och informerar mottagarna om dokumentet har ändrats eller inte efter det att undertecknaren signerade dokumentet.

För att kunna signera ett dokument krävs ett s.k. elektroniskt ID som kan liknas vid ett elektroniskt körkort eller pass som bevisar en persons identitet.

5 Genomförande

5.1 Tvåfaktorautentisering

N.B. En tjänst för tvåfaktorautentisering som är integrerad med universitetets gemensamma inloggningstjänst (AKKA) är planerad för utveckling och införande under2015-2016.

5.2 Kryptering och signering av e-post

Se *Bilaga 2 – Instruktion för kryptering och signering av e-post.*

5.3 Elektronisk signering av dokument

Se *Bilaga 3 – Instruktion för elektronisk signering av dokument.*

6 Bilagor

Bilaga 2 – Instruktion för kryptering och signering av e-post.

Bilaga 3 – Instruktion för elektronisk signering av dokument.