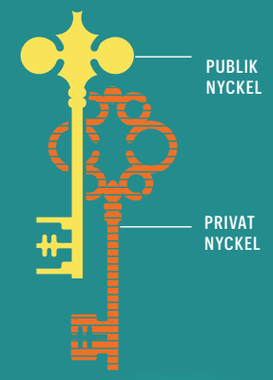
Så funkar ditt Bank-id

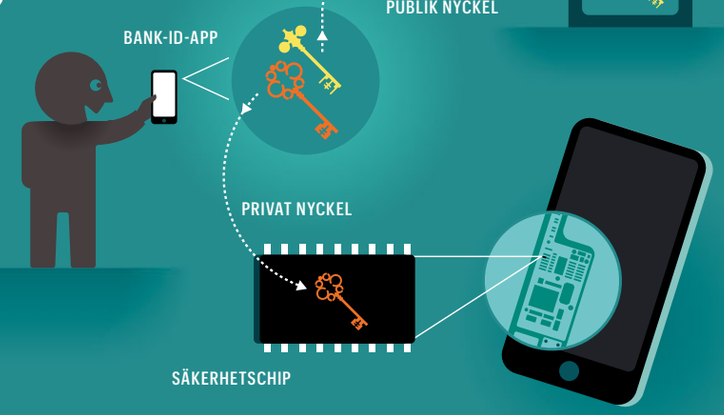
ASYMMETRISK KRYPTERING

1 | Så kallad asymmetrisk kryptering är en av de vanligaste och viktigaste principerna för att skydda hemligheter på internet. Den baseras på par av krypteringsnycklar där bara den ena nyckeln, den privata, behöver vara hemlig. Den andra, publika nyckeln kan spridas fritt, vilket är en stor fördel. Krypteringen bygger på en matematisk asymmetri som innebär att det är lätt att multiplicera två stora primtal, men mycket tidsödande att gå åt andra hållet och utifrån produkten försöka räkna ut vilka två primtal som använts.



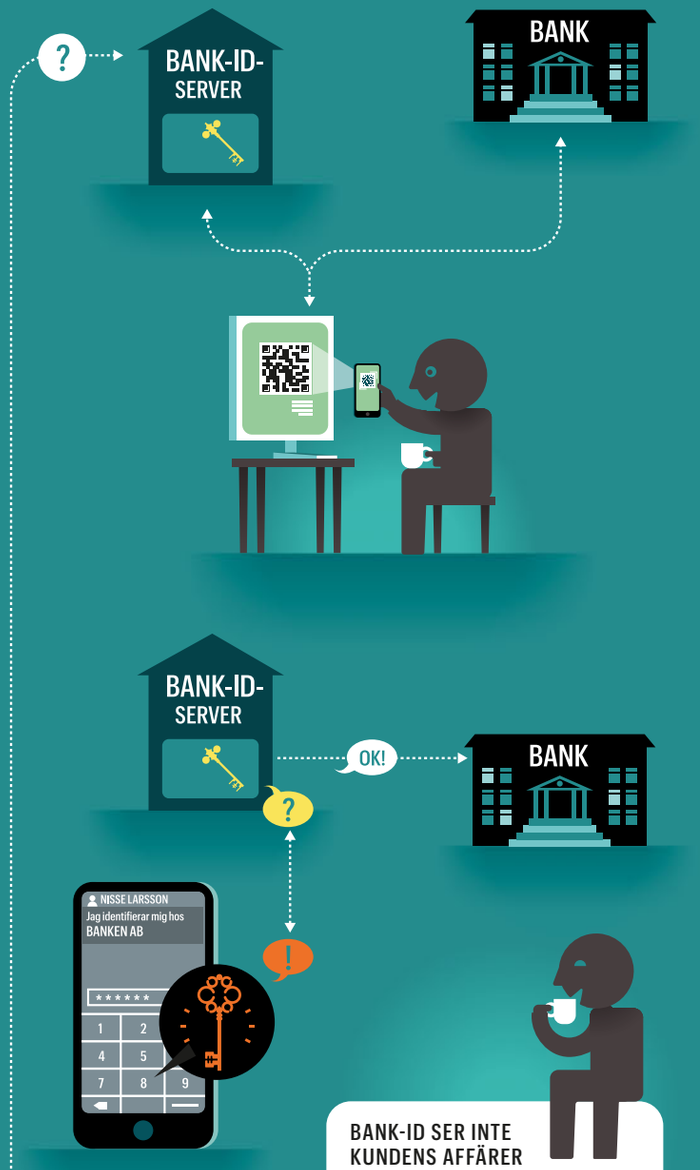
BANK-ID INSTALLERAS

2 | När en kund installerar ett nytt mobilt Bank-id på sin mobil skapas ett asymmetriskt nyckelpar: en privat nyckel som lagras på telefonen och en publik som lagras i Bank-id:s server. Den privata nyckeln skyddas i mobilens säkerhetschip – en separat del av hårdvaran för förvaring och hantering av koder. Den kod som kunden väljer (eller ibland kundens fingeravtryck eller ansikte) är det enda sättet att få tillgång till den privata nyckeln.



INLOGGNING

3 | När kunden surfar in på bankens webb och vill logga in är det första som händer att kommunikationen krypteras så att den inte kan avlyssnas. Banken skickar en förfrågan till Bank-id.



QR-KOD KNYTER IHOP

4 | Om kunden sitter vid datorn men använder mobilt Bank-id kan en QR-kod visas på datorskärmen. När kunden skannar QR-koden med sin mobil vet Bank-id att datorn och mobilen är på samma plats. Inloggning med QR-kod förhindrar bedrägerier där kunden blir lurad att logga in åt en annan person på en annan plats.

SKYDDAD MJUKVARA

5 | Bank-id-appen ska kunna stå emot intrång och till exempel upptäcka om en mobils operativsystem har manipulerats. Hur detta skydd är konstruerat hör till de hemligheter som Bank-id av säkerhetsskäl inte går närmare in på. Generellt har mobilappar svårt att avlyssna varandra på grund av så kallad *sandboxing* – en princip som innebär att alla appar, för att inte störa varandra, körs i var sin separat del av minnet.

VERIFIERING

6 | Nu är det dags för själva kontrollen. Kunden slår sin kod (eller använder fingeravtryck eller ansikte) vilket låser upp kundens privata nyckel i mobilen. Den privata nyckeln lämnas aldrig ut. Den bevisar i stället sin äkthet genom att klara ett krypteringsuppdrag som Bank-id skickar. Om det svar som den privata nyckeln skickar tillbaka till Bank-id kan dekrypteras med den publika nyckeln så har nyckelparet klarat kontrollen.

BANK-ID SER INTE KUNDENS AFFÄRER

7 | Bank-id meddelar banken att kunden kunnat identifiera sig. Eftersom kund och bank även har direktkontakt får Bank-id aldrig insyn i kundens affärer. Bara den text som ska visas i Bank-id-appens fönster passerar Bank-id men den sparas inte.

VAR FÖRSIKTIG

Att tekniken är säker hjälper inte om bedragare lyckas lura människan som använder tekniken. Lämna aldrig ut koder till någon annan, och använd inte Bank-id på uppmaning av någon annan. Kontrollera var du identifierar dig eller vad du skriver under genom att alltid läsa texten som visas i appen. Är du osäker, välj avbryt. Misstänker du bedrägeri, spärra ditt Bank-id, kontakta banken och gör polisanmälan.

KÄLLA/FAKTAKOLL: FINANSIELL ID-TEKNIK/BANK-ID

Forskning & Framsteg

Illustration: Johan Jarnestad