Nasjonal sikkerhetsmyndighet

IT-veiledning for ugraderte systemer nr. 16 (U-16).
Oppdatert: 2016-10-13

Universal 2nd Factor (U2F)

Brukerautentisering mot nettsteder

Hvordan oppnå tilfredsstillende autentisering av brukere ved hjelp av standardisert to-faktor autentisering.

Dette dokumentet beskriver hvordan U2F virker og hvordan denne protokollen skal benyttes for å sikre brukerautentisering mot nettsteder.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20. mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 814
1306 Sandvika

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09

Militær telefon/telefaks
515 40 00/515 40 09

Webadresse
nsm.stat.no

E-postadresse
post@nsm.stat.no

Innhold

1 Innledning

Autentisering av brukere er en forutsetning for å tilby tjenester til tiltenkte brukere. To-faktor autentisering er autentisering med noe man vet og noe man har. Noe man vet er som regel passord. Dette har til nå vært enerådende, men det har medført en rekke forfalskede påloggingger og dermed kompromitteringer av både bedrifts- og personsensitiv informasjon. Ved å benytte noe man har i tillegg til noe man vet, gjør man det vanskeligere for angripere å utgi seg som den tiltenkte brukeren. Foruten at nettstedet på denne måten kan være sikrere på at kun de tiltenkte brukerne benytter tjenestene, vil brukerne kunne benytte passord som er lettere å huske for nettstedet.

For å tilby to-faktor autentisering, må man sørge for at både nettsted og brukere har støtte for og benytter samme mekanisme. *Universal 2nd Factor* (U2F) er en åpen protokoll for to-faktor autentisering. Denne protokollen er støttet både i enkelte nettlesere, på store nettsteder og for en rekke publiseringssystem. Fysiske sikkerhetsnøkler som ikke er kopierbare, hindrer en rekke angrep mot passord og gir beskyttelse mot avlytting.

NSM anbefaler at flest mulig nettsteder med brukerpålogging tilbyr to-faktor autentisering ved hjelp av U2F-protokollen og fysiske sikkerhetsnøkler.

Denne veiledningen beskriver hvorfor man bør benytte to-faktor autentisering, hvordan U2F fungerer og hvorfor denne protokollen bør benyttes. Kontaktpunkt for veiledningen er post@nsm.stat.no. Vennligst bruk veiledningens navn som emne. Kommentarer og innspill mottas med takk.

2 Om U2F

Universal 2nd Factor (U2F) er en åpen standard for to-faktor autentisering mot nettsteder ved hjelp av sikkerhetsnøkler. Sikkerhetsnøklene kan være program- eller maskinvarebaserte. Standarden forvaltes av Fast IDentity Online-alliansen (FIDO) som består av anerkjente aktører som Google, Intel, Lenovo, Microsoft, NXP, PayPal og Samsung.

Produkter og tjenester som er testet å virke med U2F kalles *FIDO Ready*, og sertifiserte løsninger som gjennomgår ekstra sikkerhetstesting kalles *FIDO Certified*[1]. Nettsteder som støtter U2F inkluderer[2] , Dropbox, Google, GitHub, GitLab, Fastmail, StrongAuth og Wordpress.

Fysiske sikkerhetsnøkler selges blant annet av Yubico[3], Hypersecu Information Systems[4] og Feitian Technologies[5].

For å benytte U2F må nettleseren ha støtte for protokollen. Til nå har Chrome integrert støtte, mens Firefox har støtte via utvidelse (*plugin*). Dette betyr at alle relevante plattformer har tilgjengelig nettleser med støtte for U2F. Samtidig jobber FIDO-alliansen med W3C[6] (standardiseringsorganet for web) for å få integrert U2F-støtte i andre nettlesere.

U2F bruker *challenge response* (godkjenningsspørsmål) basert på offentlig nøkkelkryptering i sikkerhetsnøkkel, for å verifisere at det er tiltenkte bruker som ønsker tilgang.

For å ta i bruk U2F mot et nettsted må sikkerhetsnøkkelen først registreres hos nettstedet. Dette gjøres kun én gang for hver sikkerhetsnøkkel man ønsker å bruke. Ved registrering, genererer sikkerhetsnøkkelen følgende:

- **Nøkkelpar** – Et kryptografisk nøkkelpar bestående av en *privat* og *offentlig nøkkel*.
- **Nøkkelidentifikator** – Identifikator til hvilken nøkkel som brukes mot nettstedet.

Den offentlige nøkkelen og nøkkelidentifikatoren sendes til nettstedet man registrerer seg for.

Det er mulig å registrere flere sikkerhetsnøkler til samme nettsted og samme sikkerhetsnøkkel til flere nettsteder. Dette er hensiktsmessig både for brukere som har ulike sikkerhetsnøkler og for brukere som har flere brukerkontoer på en tjeneste.

Autentisering ved bruk av U2F og sikkerhetsnøkkel skjer i tre faser (oppkobling, signering og verifikasjon) og utføres av tre parter (sikkerhetsnøkkel, nettleser og nettsted)

[1] https://fidoalliance.org/certification/fido-certified/

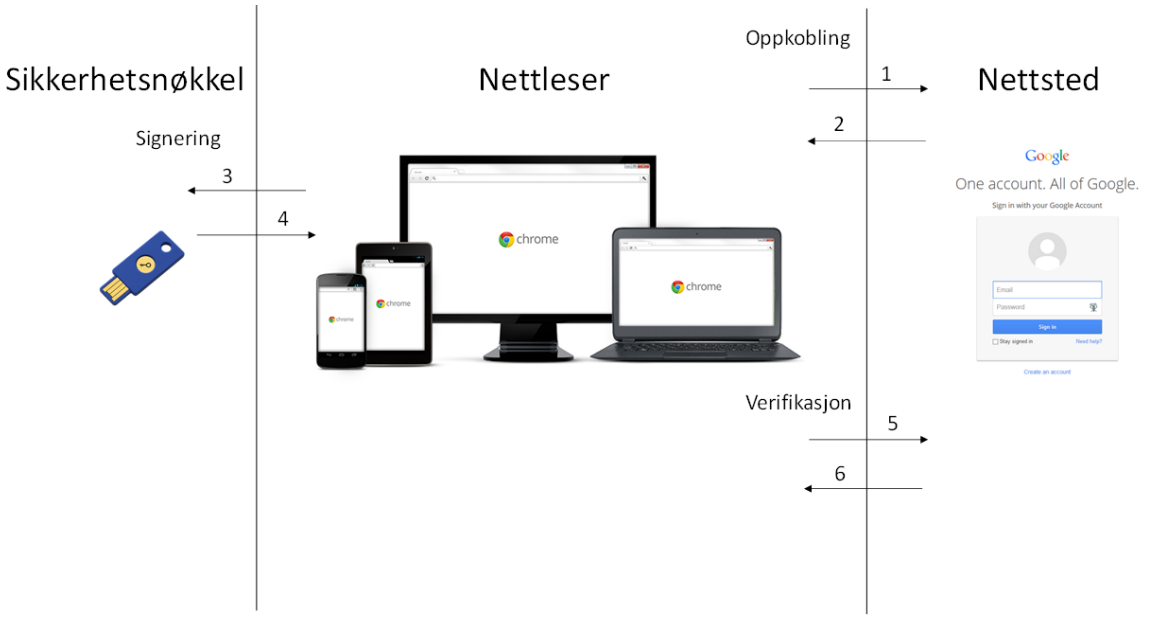
[2] http://www.dongleauth.info/

[3] https://www.yubico.com/products/yubikey-hardware/

[4] https://hypersecu.com/products/hyperfido

[5] http://www.ftsafe.com/products/FIDO

[6] https://www.w3.org/



Ved oppkobling kontakter nettleseren nettstedet (1) og får tilsendt nøkkelidentifikatoren og et godkjenningsspørsmål (2). Godkjenningsspørsmålet sendes sammen med nøkkelidentifikatoren og avtrykket av nettstedets adresse til sikkerhetsnøkkelen. Sikkerhetsnøkkelen kan dermed verifisere at autentiseringsforespørselen kommer fra en tjeneste den allerede er registrert mot. I tillegg til nøkkelidentifikator og godkjenningsspørsmål, kan nettleseren legge inn ytterligere informasjon inn i meldingen som skal signeres av sikkerhetsnøkkelen.

Meldingen fra nettleseren sendes så til sikkerhetsnøkkelen (3) hvor den signeres. Sikkerhetsnøkkelen signerer meldingen og sender dette tilbake til nettleseren (4).

Nettleseren sender svaret videre til nettstedet (5), hvor signaturen verifiseres mot brukerens offentlige nøkkel. Dersom meldingen er autentisk, slippes brukeren videre inn i prosessen eller inn på nettstedet (6).

2.1 Alternativer til U2F

Det finnes en rekke ulike to-faktor autentiseringsløsninger tilgjengelig for nettbaserte tjenester. De fleste av disse er proprietære og lukkede. «Logg inn med QR-kode» er et eksempel på en slik løsning, men disse er ikke gode alternativer til U2F da de har begrenset støtte på tvers av nettsteder.

En annen gruppering av anerkjente aktører kalt *Initiative for Open Authentication* (OATH)[7] har spesifisert to protokoller for to-faktor autentisering. Disse protokollene, *HMAC-based One-Time Password* (HOTP) og *Time-based One-Time Password* (TOTP), er spesifisert i henholdsvis RFC 4226[8] og RFC 6238[9]. Protokollene er like, med unntaket av at HOTP bruker en teller (tall) og TOTP bruker tid for å

[7] https://openauthentication.org/

[8] https://www.ietf.org/rfc/rfc4226.txt

[9] https://www.ietf.org/rfc/rfc6238.txt

generere unike autentiseringskoder. Dersom U2F ikke kan benyttes, anbefales det å benytte OATH-protokollene.

En annen, åpen standard og protokoll for to-faktor autentisering, *Secure Quick Reliable Login* (SQRL)[10] benytter mange av de samme kryptografiske prinsippene som U2F. Dessverre utvikles denne protokollen av bare en person og den har dermed ikke like høy tillit som U2F.

Det bør for øvrig unngås å benytte protokoller med lav tillit til faktorene (som fingeravtrykk og lyd-opptak) eller med lav tillit til overføringsmekanismene (som SMS og epost).

[10] https://www.grc.com/sqrl/sqrl.htm

3 Anbefalte tiltak

3.1 Benytt to-faktor autentisering

NSM anbefaler at flest mulig nettsteder med brukerpålogging tilbyr to-faktor autentisering.

To-faktor autentisering er autentisering med noe man vet og noe man har. Tradisjonelt autentiserer brukere seg med noe de vet, nemlig et passord. Dessverre er ikke passord sterk nok mekanisme til å hindre uautorisert autentisering.

Fordi passord skal huskes, er de som regel korte, i tillegg til at en rekke kompromitteringer av passorddatabaser har gitt angripere informasjon om hvilke passord som benyttes. På denne måten kan man enkelt prøve å logge på som en bruker ved å teste vanlige passord. Når uvedkommende autentiserer seg på en nettjeneste, blir både den tiltenkte brukeren og nettstedets informasjon kompromittert.

3.2 Benytt Universal 2nd Factor (U2F)

NSM anbefaler to-faktor autentisering mot nettsteder ved hjelp av U2F-protokollen.

U2F er en åpen protokoll og dermed kan sikkerhetsmekanismene verifiseres av uavhengige parter. I tillegg er det ingen begrensninger i bruken av protokollen. Per oktober 2016 har verken U2F-protokollen eller anerkjente implementasjoner av denne noen kjente sårbarheter.

Protokollen støtter at flere uavhengige nettsteder kan benytte samme sikkerhetsnøkkel slik at brukerne bare trenger å forholde seg til én sikkerhetsnøkkel. Selv med samme sikkerhetsnøkkel vil hvert nettsted benytte unike nøkler. I praksis er det ingen begrensninger for hvor mange nettsteder en sikkerhetsnøkkel kan assosieres med.

Ved å standardisere på U2F-protokollen oppnår man variantbegrensning. Dette betyr at nettstedene ikke må forholde seg til mange ulike autentiseringsmekanismer, noe som reduserer implementasjonskompleksiteten og angrepsflaten. I tillegg øker brukervennligheten fordi innloggingsprosedyren blir lik på tvers av tjenester, brukerne kan benytte passord som er enkle å huske, og fordi brukerne bare må passe på én sikkerhetsnøkkel.

U2F gir også økt sikkerhet ved å forhindre *Man in the Middle*-angrep. Avtrykket av nettstedets adresse som sendes til sikkerhetsnøkkelen ved autentisering hindrer falske nettsteder å gjennomføre autentiseringer på vegne av brukeren. I tillegg kan nettleseren legge inn *TLS Channel ID* i meldingen (*Request Message*) som signeres av sikkerhetsnøkkelen. Dermed rapporteres det om eventuelle andre TLS-kanaler som benyttes mellom nettleseren og nettstedet. Sistnevnte er en opsjon i U2F-protokollen, men NSM anbefaler at denne benyttes.

3.3 Benytt fysisk sikkerhetsnøkkel

NSM anbefaler at U2F benyttes med fysiske sikkerhetsnøkler.

Fysiske sikkerhetsnøkler er laget for å sikre hemmeligheter. Ved å benytte en fysisk sikkerhetsnøkkel hindrer man muligheten for at uvedkommende skal hente ut de kryptografiske nøklene i denne og dermed kunne autentisere seg på vegne av den tiltenkte brukeren.

Fysiske sikkerhetsnøkler krever at brukeren er til stede før autentiseringen gjennomføres. Dette gjøres typisk ved hjelp av en fysisk trykknapp og hindrer programvarebaserte angrep (skadevare) fra å gjøre autentisering uten brukerens viten og vilje. Dermed kan man la sikkerhetsnøkkelen stå inne i datamaskinen til enhver tid, uten at den kan misbrukes av uvedkommende på Internett. De fysiske egenskapene til sikkerhetsnøkkelen og trykking på knappen hindrer automatiserte masseforsøk (*brute force*-angrep).

Det er ikke nødvendig at sikkerhetsnøkkelen benyttes for hver autentisering. Avhengig av konfigurasjon på nettsted, kan man velge hvor ofte og for hvilke tilgangsnivåer brukeren må autentisere seg ved hjelp av sikkerhetsnøkkelen.

Både USB, NFC og Bluetooth er støttet som grensesnitt mot fysiske sikkerhetsnøkler. På denne måten er både stasjonære, bærbare og mobile enheter støttet.

Formfaktoren til flere fysiske sikkerhetsnøkler er lik husnøkler. Siden tilgang til det digitale livet er like viktig som det fysiske, bør sikkerhetsnøkler håndteres på samme måte og festes på nøkkelknippet.

Noen fysiske sikkerhetsnøkler tilbyr også funksjonalitet utover U2F-protokollen. For avanserte brukere eller bedrifter med ønske ytterligere sikkerhetsfunksjonalitet, kan slike sikkerhetsnøkler benyttes. Funksjonalitet utover U2F kan være:

- Smartkort for PKI-basert to-faktor autentisering, filkryptering og epost-signering
- Nøkkellager for OpenPGP og SSH
- HOTP og TOTP
- Pålogging til programvare for passordhåndtering

3.4 Etabler sikker gjenopprettingsmulighet

NSM anbefaler å etablere sikre gjenopprettingsmuligheter i tilfelle tap av sikkerhetsnøkkel.

For å hindre at tap av sikkerhetsnøkkelen ikke sperrer brukeren ute fra nettsteder, anbefales det å konfigurere gjenopprettingsløsning for kontoene. Dessverre har gjenopprettingsløsninger i mange tilfeller blitt brukt av uvedkommende for å få tilgang til informasjon. Det er derfor viktig at man ikke benytter gjenopprettingsløsninger som er svakere enn vanlig autentiseringsmekanisme. Statiske passord som kan benyttes flere ganger, gjenoppretting via epost eller SMS, og sikkerhetsspørsmål bør derfor unngås.

Eksempler på gode gjenopprettingsmuligheter er:

Registrér to sikkerhetsnøkler for hver tjeneste. Dersom man har flere sikkerhetsnøkler, kan man benytte den andre, når man mister den første. Dette kan også løses ved at man registrerer både egen og en tiltrodd kollega/venn sin sikkerhetsnøkkel mot samme nettsted. Vedkommende vil ikke få tilgang til nettstedet siden man har individuelle passord.

Skriv ut gjenopprettingspassord. Noen nettsteder tilbyr å generere og skrive ut gjenopprettingspassord. Dette er svært komplekse passord som kun kan benyttes én gang når man har blitt sperret ut fra nettstedet. For å hindre misbruk, må dette passordet oppbevares på et trygt sted, gjerne annet sted enn hjemmet.

Vedlegg A Dokumenthistorikk

2016-09-01 Dokumentet ble opprettet.

2016-09-27 Intern høring.

2016-10-01 Publisering.