Slutrapport tvåfaktorsautentisering

på uppdrag av Inkubator

1

Innehåll

2 INLEDNING 3
2.1 DEFINITIONER AV BEGREPP 3
2.2 MÅL 4
2.3 TIDPLAN 4
2.4 KOSTNADER 4
2.5 DOKUMENTATION 4
3 ORGANISATION 5
3.1 UPPDRAGSGIVARE 5
3.2 REFERENSGRUPP 5
3.3 PROJEKTGRANSKARE 5
3.4 PROJEKTLEDARE 5
3.5 RESURSPERSONER 5
4 GENOMFÖRANDE 6
4.1 ”KARTLÄGGNING OCH BEHOVS ANALYS AV TVÅFAKTORSAUTENTISERING VID LÄROSÄTEN” 6
4.2 RESULTATET AV ENKÄTEN SOM SKICKADES UT 7
4.3 PRODUKTGENOMGÅNG AV LOKALT IMPLEMENTERINGSBARA LÖSNINGAR 10
4.4 NATIONELLT IMPLEMENTERAD LÖSNING AV TVÅFAKTORSAUTENSISERING OCH SAML2 27
5 SAMMANFATTNING 30
6 REKOMENDATIONER FÖR FORTSATT ARBETE 32
6.1 LÖSNINGAR SOM INTE GÅTT VIDARE I PROJEKTET 32

2 INLEDNING

Behovet av en ökad säkerhet kring olika typer av inloggningar via internet har ökat och ett sätt att hantera det är att i större utsträckning använda sig av tvåfaktorsautentisering. SWAMI har sedan tidigare arbetat med området tvåfaktorautentisering och ett antal aktiviteter är redan påbörjade.

SUNET Inkubator avser att fortsätta det arbetet genom att kartlägga vilka metoder som idag används för tvåfaktorautentisering och vilka som skulle kunna vara intressanta på svenska lärosäten. En genomlysning av marknaden genomförs för att hitta vad som finns inom området både nationellt och internationellt, t.ex. det arbete som görs på SURFnet. POC (proof os concept) ska tas fram över särskilt intressanta metoder.

Den här slutrapporten innehåller rekommendationer som rör hanteringen av tvåfaktorautentisering vid svenska lärosäten.

Delar av rapporten är på engelska eftersom att det utvärderats av en engelskspråkig person.

2.1 DEFINITIONER AV BEGREPP

IdP Identity Provider.

Proxy-IdP En IdP som i sin tur anropar andra IdP:er. En fördel är att man kan lägga till eller ta bort information. En SP kan i sin request ange vilka IdP:er som får användas.

RA Registration Authority, En registreringsmyndigheten (RA) är en enhet som är betrodd att registrera eller gå i god för identiteten hos användare. En RA fokuserar på att identifiera och autentisera användare.

SMS-OTP Ett engångslösenord (One Time Password) skickas med SMS till användarens registrerade mobilnummer.

SP Service Provider.

SURFnet Nederländernas motsvarighet till svenska SUNET.

tiqr En inkloggningsmetod för mobiler (Android och iOS) utvecklad av SURFnet. Man får upp en QR-kod som man scannar in med telefonen varefter man anger en PIN-kod.

Yubikey En USB-sticka som genererar slumpmässiga engångslösenord och simulerar ett tangentbord. Tillverkas av det svenska företaget Yubico.

AD Active Directory är en katalogtjänst från Microsoft som innehåller information om olika IT-resurser inom en organisation t.ex, datorer, skrivare och användare.

Federationstyper

Hub and spoke En central IdP som alla SP (Service providers) jobbar mot. Den centrala IdP:n kan vara en proxy-IdP som i sin tur anropar högskolornas egna IdP:er eller LDAP-kataloger. Modellen används av Nederländerna, Danmark och Norge.

Full Mesh Man har ingen central IdP utan samtliga IdP:s och SP:s håller reda på

varandra med hjälp av en centralt utdelad metadatafil.

2.2 MÅL

Det finns fyra delmål:

1. Genomföra en kartläggning angående vad som används rörande tvåfaktorsautentisering på svenska lärosäten.
2. Gör en teknisk genomlysning av möjliga verktyg kopplat till tvåfaktorsautentisering.
3. Genomför en POC över intressanta metoder.
4. Ta fram dokumenterade rekommendationer för tvåfaktorsautentisering.

2.3 TIDPLAN

Projektet startas 2013-02-01 och avslutas 2013-12-31

2.4 KOSTNADER

Aktiviteter	Resurs	Budget 2013(timmar)
Utredningsarbete	Joakim Nyberg	
Genomlysning verktyg	Joakim Nyberg, Jan Pettersson, Einar Hillbom & Enrico Pelletta	
POC	Joakim Nyberg, Jan Pettersson & Einar Hillbom	
Totalt		400

2.5 DOKUMENTATION

- Fastställd projektplan
- Statusrapporter
- Slutrapport

3 ORGANISATION

3.1 UPPDRAGSGIVARE

Inkubator är uppdragsgivare och Per Högblad kontaktperson

3.2 REFERENSGRUPP

Gruppen består av ett antal representanter från svenska för lärosätena.

ANDERS LÖRDAL	HÖGSKOLAN I GÄVLE
ANDREAS JONASSON	CHALMERS
DAVID HEED	ÖREBRO UNIVERSITET
FREDRIK THULIN	SUNET
HANS CARLBRING	UPPSALA UNIVERSITET
JOHANNES HASSMUND	LINKÖPINGS UNIVERSITET
LEIF JOHANSSON	SUNET
LEIF LAGEBRAD	BLEKINGE TEKNISKA HÖGSKOLA
PER HÖRNBLAD	UMEÅ UNIVERSITET
PIA SKOTARE	SVENSKA LANTBRUKSUNIVERSITETET
TORBJÖRN WICTORIN	UPPSALA UNIVERSITET

3.3 PROJEKTGRANSKARE

Projektgranskning sker av Per Hörnblad, IT-arkitekt, Umeå universitet

3.4 PROJEKTLEDARE

Projektledare är Joakim Nyberg, IT-stöd och systemutveckling, ITS, Umeå universitet

3.5 RESURSPERSONER

Einar Hillbom – ITS, Umeå universitet

Jan Pettersson – ITS, Umeå Universitet

Enrico Pellet – Kungliga Tekniska Högskolan

4 GENOMFÖRANDE

4.1 ”KARTLÄGGNING OCH BEHOVS ANALYS AV TVÅFAKTORSAUTENTISERING VID LÄROSÄTEN”

Enkäten skickades ut till IT-chefer vid svenska lärosäten.

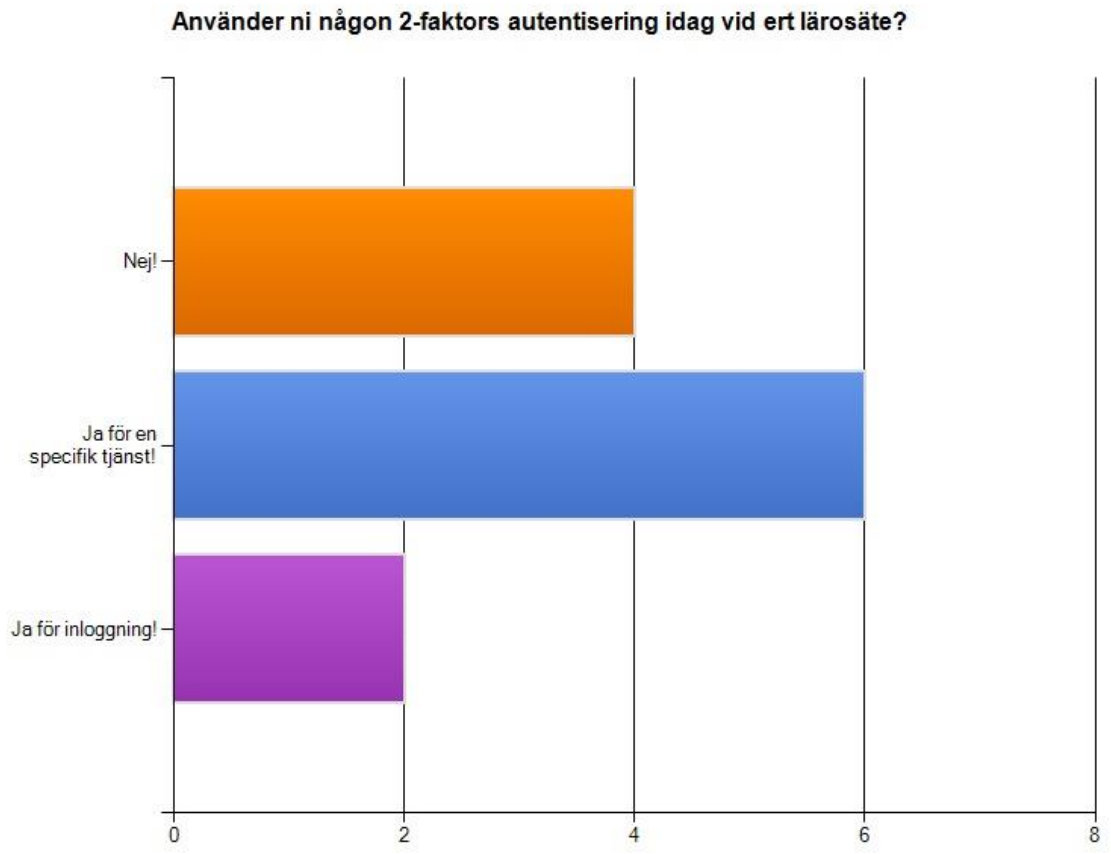
Elva lärosäten svarade på enkäten:

1. Blekinge Tekniska Högskola
2. Chalmers
3. Handelshögskolan i Stockholm
4. Högskolan i Borås
5. Högskolan i Gävle
6. Karlstads universitet
7. Karolinska Institutet
8. Lunds universitet
9. Stockholms universitet
10. Södertörns högskola
11. Umeå universitet

4.2 RESULTATET AV ENKÄTEN SOM SKICKADES UT

Här följer en sammanställning av de frågor som enkäten innehöll.

1. **Använder ni någon tvåfaktorsautensiering idag vid ert lärosäte?**



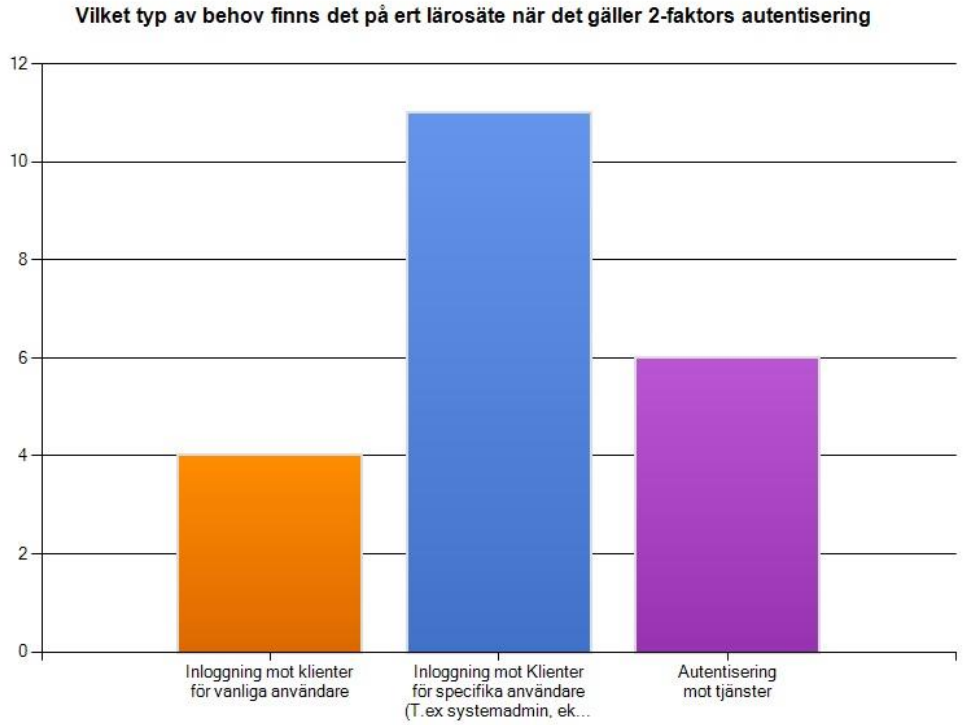
2. Om ni har svarat på frågan F1 med ett svar som har ett ja i sig så beskriv kort hur det används!

- Lunarc (HPC-klustren inom SweGrid) använder idag 2-faktors autentisering och vi har även haft pilotverksamhet för domain-admin.
- Används för administrativinloggning i känsliga system
- Vi har börjat använda 2-faktors autentisering för systemadmin access till centrala Linux servrar som en pilot. Vi använder oss Yubikey. Vår Nätverksgruppen är intresserad av att börja använda Yubikey med switcher/routers osv.
- Känslig applikation kräver en extra pinkod via mobil vid användning på distans
- Attestering av utbetalningar i ekonomisystemet
- Inloggning till VPN för distans access till interna system
- Det används internt hos ITS för vissa känsliga system. Beroende på hur 2-faktor definieras tillämpas en enklare variant för betalattestering i fakturahanteringen.

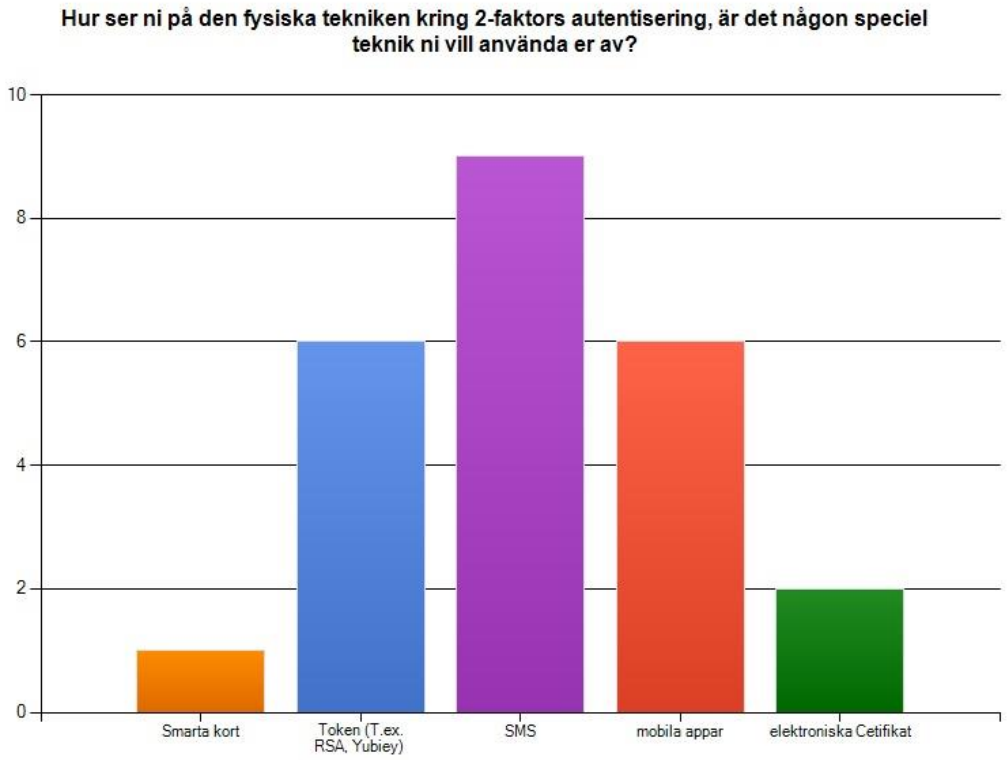
3. Ser ni några brister och/eller problem med den eller dom lösningarna ni i dag använder?

- Inte direkt.
- Den lösningen som vi testa fungera f.n på bara en del av våra servrar (Centos/Red Hat 6). Äldre servrar har inte stöd i openssh för flera faktors login. Det löser sig själv över tid.
- Speciallösning för en applikation
- Kräver separat dosa
- Nej egentligen inte, den kan även användas för 2 faktorsautentisering till tex inloggning på servrar.
- Inte vad jag har hört, men jag är heller inte insatt.

4. Vilken typ av behov finns det på ert lärosäte när det gäller tvåfaktorsautentisering



5. Hur ser ni på den fysiska tekniken kring 2-faktors autentisering, är det någon speciel teknik ni vill använda er av?



6. Vad förväntar ni er av Inkubators 2-faktors autentisering projekt!

- Jag vet för lite
- Rekommendationer av verifierade tekniska lösningar anpassade att sprida till användare i större skala.
- Att få hjälp att bedöma om vald lösning är den bästa för ändamålet och att eventuellt få rekommendationer till ett bättre alternativ.
- En stabil tjänst som är enkel att applicera för olika tillämningar. Vi skulle gärna se en lösning som använder bankID då i stort sett alla stundenter har ett bankID idag, likväl som stora delar av den gemena befolkningen. Den lösningen ser vi helst en satsning mot.
- Use cases, best practices - hur 2-faktors autentisering skulle kunna skala till större grupper av användare.
- En standardiserad lösning som utvecklas i takt med de hotbilder som kommer att finnas
- Ett förslag på en välfungerande, användarvänlig och kostnadseffektiv lösning.
- En bra, enkel, säker och billig lösning :)

4.3 PRODUKTGENOMGÅNG AV LOKALT IMPLEMENTERINGSBARA LÖSNINGAR

Inom Sunet har det framkommit önskemål om att göra en utredning för att se över vilka produkter som finns på marknaden för tvåfaktorsautentisering. Målet med utredningen är att belysa de olika produkternas styrkor och svagheter och komma med en rekommendation om hur tvåfaktorsautentisering ska hanteras inom Sunet.

En enkät har skickats ut för att få fram vilka produkter som används inom Sunet och hur de används. Det har sedan gjorts en genomgång över vilka produkter som finns tillgängliga på marknaden idag. Fem produkter har valts ut för att titta närmare på:

1. **Safenet Authentication Service**. En molnbaserad lösning som också kan köras on premises om så önskas.
2. **Mideye.** Lösning som används av Umeå kommun, Blekinge Högskola och Linköpings universitet.
3. **Authlite**. Produkt med integration mot Active Directory. Har använts inom Umeå universitet för inloggning på servermiljöer sedan en tid.
4. **Clavid - Clavid Internet Identity Provider** Autentisering och identitetshantering portal «Authentication as a Service» (AAAS) för SAML, aktiverat OpenID och OAuth Internettjänster.
5. **Microsoft Azure**. Microsoft lösning för tvåfaktorsautentisering

4.3.1 Safenet Authentication Service

http://www2.safenet-inc.com/sas/index.html

Safenet hör till ett av de ledande företagen inom tvåfaktorsautentisering idag. De har lösningar på flera olika nivåer och den vi har valt att titta på heter Authentication Service. Det är en molnlösning där man hanterar all administration av användare via ett webgränssnitt.

Teknik

I och med att det är en molnbaserad lösning så behöver inga större ingrepp göras i befintlig infrastruktur.

Användare i systemet kan antingen läggas upp manuellt i tjänsten eller synkas från en befintlig katalog som ex. Active directory (AD). Anledningen till att man vill lägga upp användare manuellt är för Linux och maskiner med lokala användarkonton.

För Active directory installeras en LDAP-klient som synkroniserar de konton som är medlem i en viss grupp i AD:t till molntjänsten. Information som synkroniseras över är kontonamn, epostadress, telefonnummer med mera. Klienten kan man sedan ställa in att synkronisera med valfritt antal minuters mellanrum beroende på hur ofta man vill ha det synkroniserat. Det går också att starta synkroniseringen manuellt vid behov.

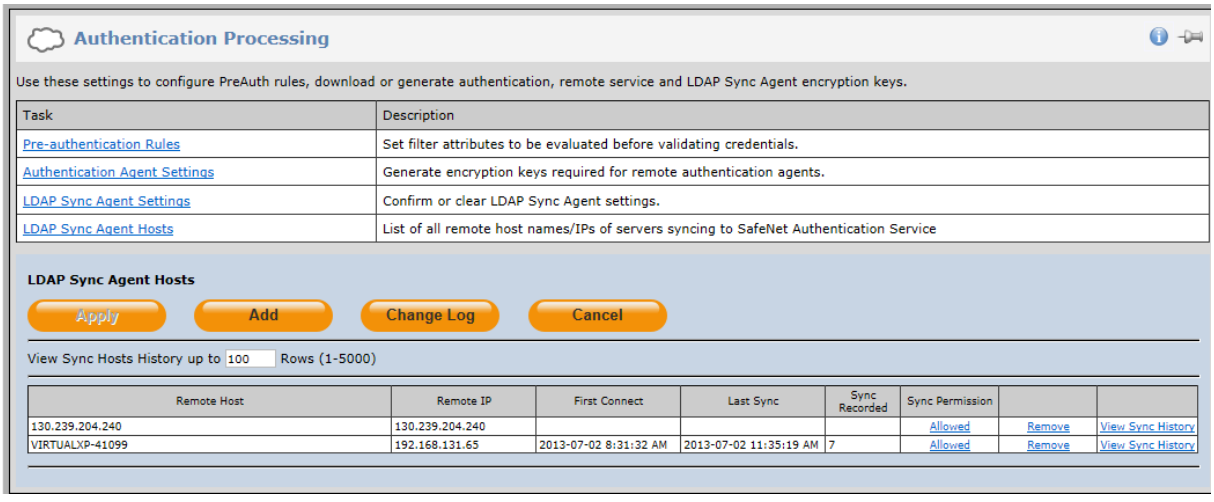
På klienterna installeras en agent som ersätter msgina.dll med en egen inloggningsprompt (Blackshield logon agent).

Plattformsstöd/Tjänster:

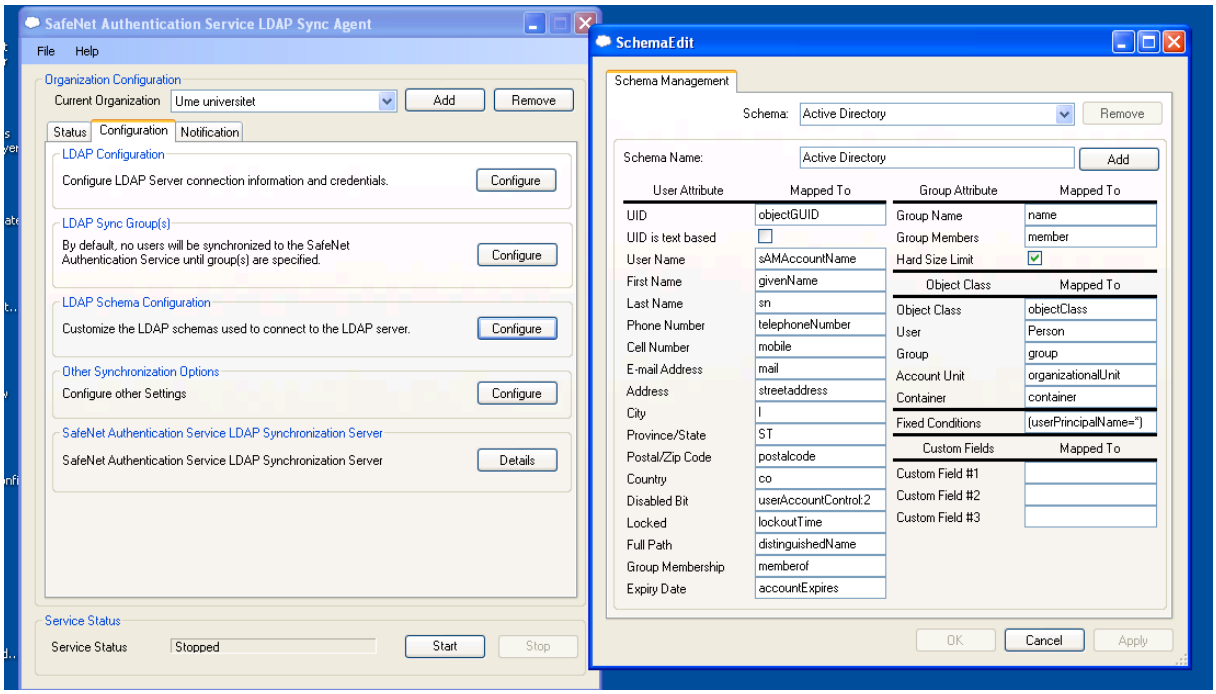
- Windows XP/2003/2008/2012 (32/64-bit)
- Cisco AnyConnect (32/64-bit)
- Citrix Web Interface 4.6 (32/64-bit)
- IIS 7 (Terminal Services Web and Remote Desktop Web)
- Juniper Steel Belted Radius
- Microsoft IIS 6.0 (OWA 2003, RWW 2003, SharePoint 2003) (32-bit)
- Microsoft Outlook Web Access 2007 and 2010 (64-bit)
- Microsoft NPS/IAS (32/64-bit)
- Remote Web Workplace (SBS 2008)
- SharePoint (SharePoint Services 3.0, Moss 2007 and SharePoint 2010)

Administration/användarhantering

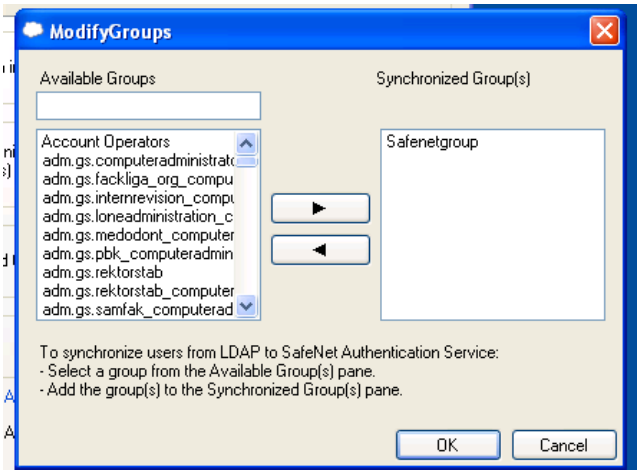
Första steget i konfigurationen är att sätta upp vilken maskin som har rätt att göra LDAP-synkroniseringar mot molnet. Själva konfigureringen av detta är inte så krånglig. Du bestämmer bara utifrån ett filter vilka konto som ska synkroniseras över. Exempelvis alla som är medlemmar i gruppen ”safenetgroup”.



Lägg till vilken host som ska få synkronisera mot tjänsten



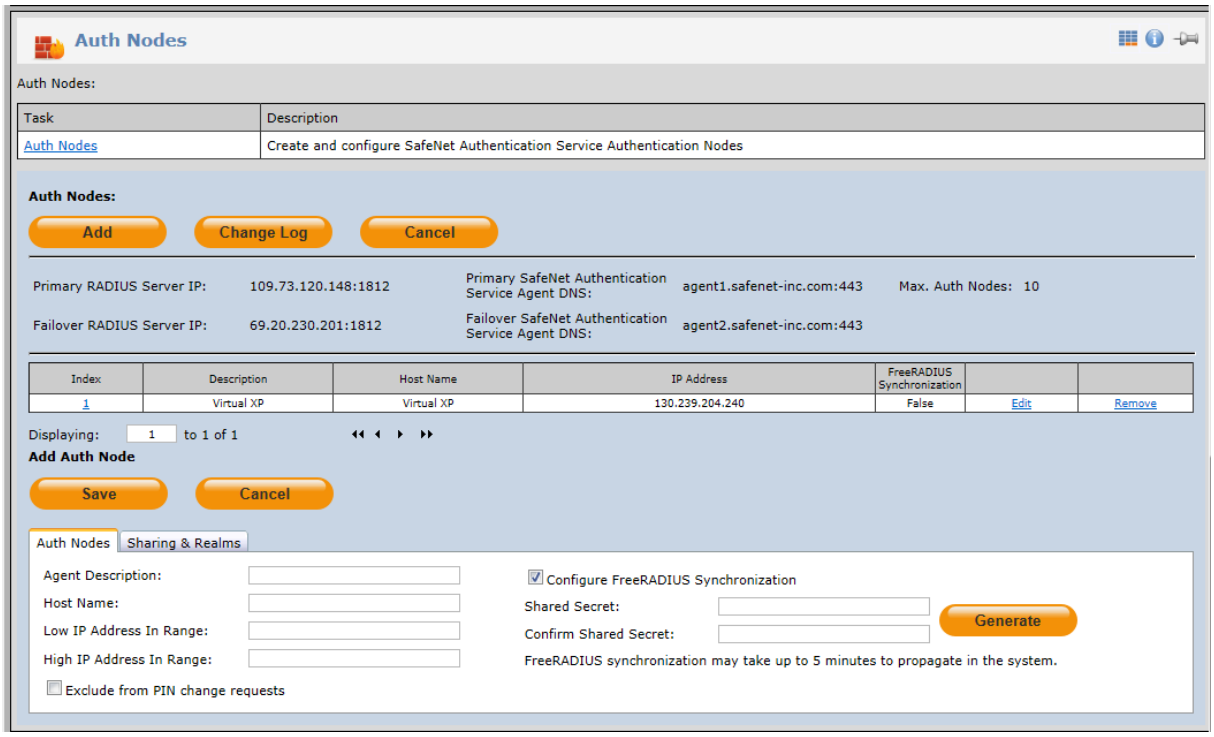
Begränsa eller lägg till vilka fält som ska synkroniseras över från LDAP-katalogen



Bestäm vilka/vilken grupp/grupper vars medlemmar ska synkroniseras över

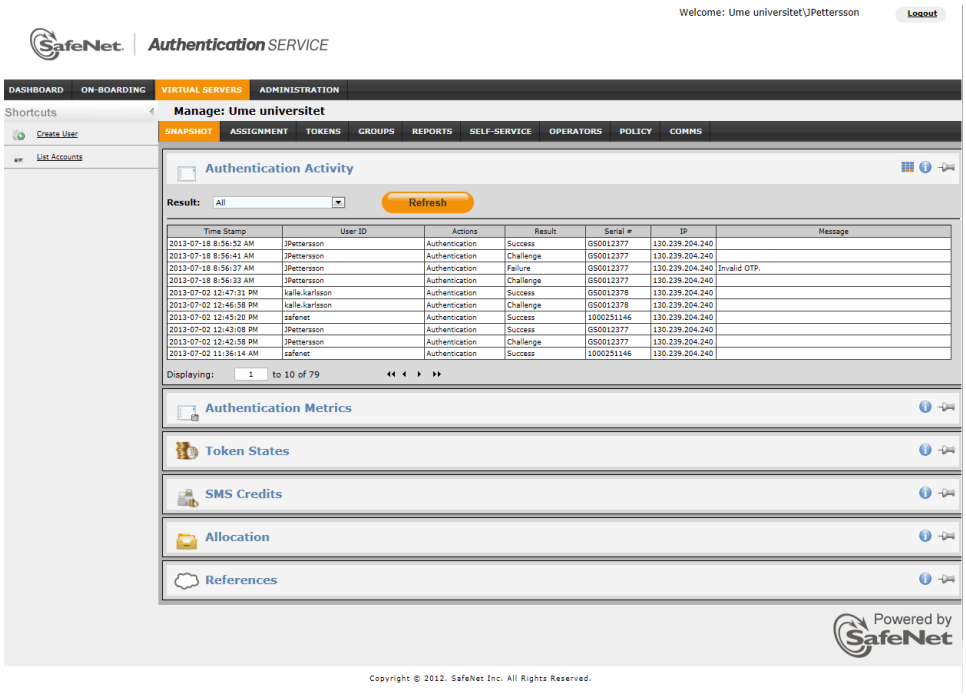
Steg två är att lägga upp vilka maskiner som ska kunna autentisera sig mot tjänsten. Tanken med detta är att koppla ihop så att tjänsten vet vilken användardatabas den ska söka efter användarna i. En maskin kan med andra ord inte kopplas till flera kunder i tjänsten, utan IP-numret ska vara unikt i hela tjänsten.

Det är även här man lägger upp autentiseringen för de maskiner som inte kan autentisera via en agent direkt, exempelvis linux och macintosh. Då måste man använda sig av en Radiusserver som i sin tur autentiserar mot tjänsten.



När man loggar in på själva tjänsten får man först en dashboard där man kan se de senaste inloggningarna och allmän status över antal licenser man utnyttjat med mera.

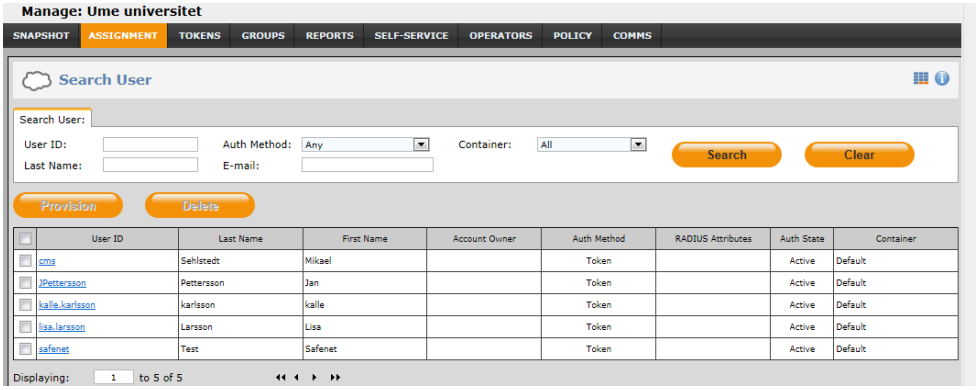
Vad man får se i gränsnittet kan anpassas så att man har administratörer i systemet med olika behörigheter. Detta skulle kunna vara en god idé ifall man vill slå ihop så att alla universitet och högskolor går under samma portal, men varje högskola eller universitet har hand om sina respektive användare. Då skulle användarna kunna vandra mellan och använda sig av sin tvåfaktorsautentisering även på andra högskolor såvida det finns en trust mellan AD-miljöerna.



I gränsnittet kan du söka upp användare och tilldela nya tokens eller nollställa om personen låst ute sitt konto eller fått en ny enhet som de behöver installera mjukvaran på.

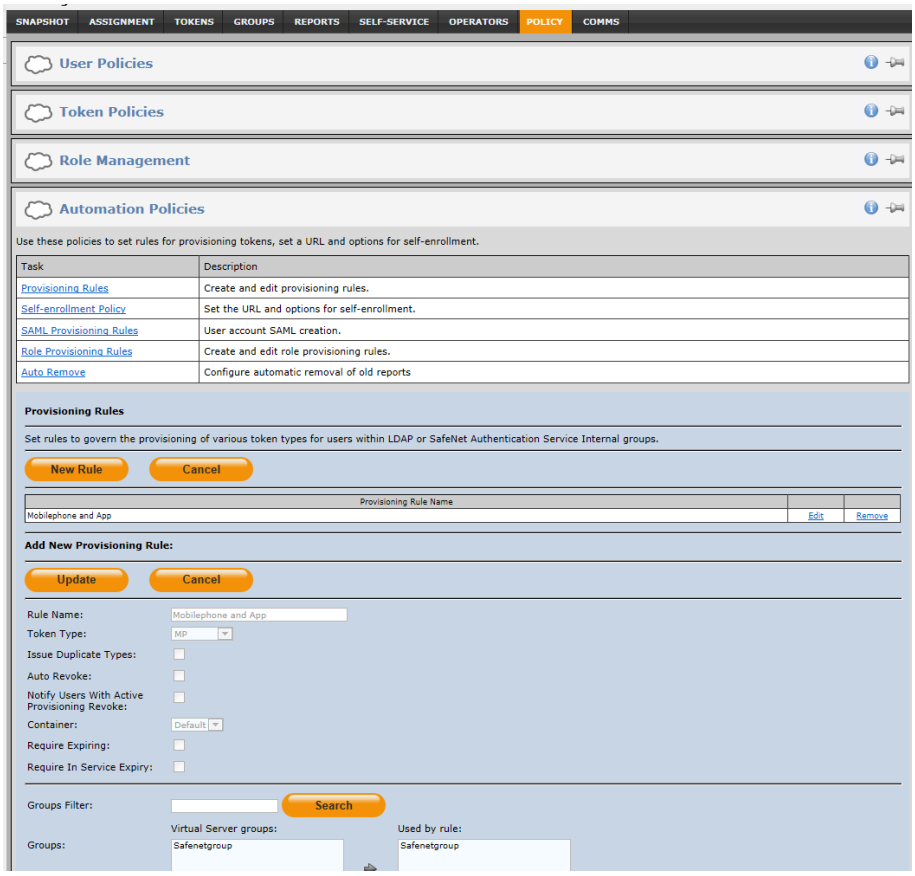
Det finns möjligheter för flera olika typers tvåfaktorsautentisering:

- **Gridsure** – Ett sifferrutmönster visas på skärmen. Fyll i de siffror som matchar ditt mönster. Fördelen är att den inte kräver extra hårdvara/mjukvara. Men det kan vara svårare att komma ihåg ett mönster än ett lösenord.
- **Token** – Slå in en fyrsiffrig kod och få tillbaka en kod som du matar in. Som en bankdosa. Kan installeras på datorn/telefonen och därmed har man med sig sin token hela tiden.
- **USB-kodnyckel**
  I och med att det är en hårdvara kan man kräva att man ska kvittera ut dessa enheter och då får man en annan sorts identitetskontroll än de övriga.
- **SMS** – Få ett sms med inloggningskod.
  Alla har mobiltelefon. Fungerar ju då även för de utan smartphone som token-varianten kräver.
- **Koddosa**

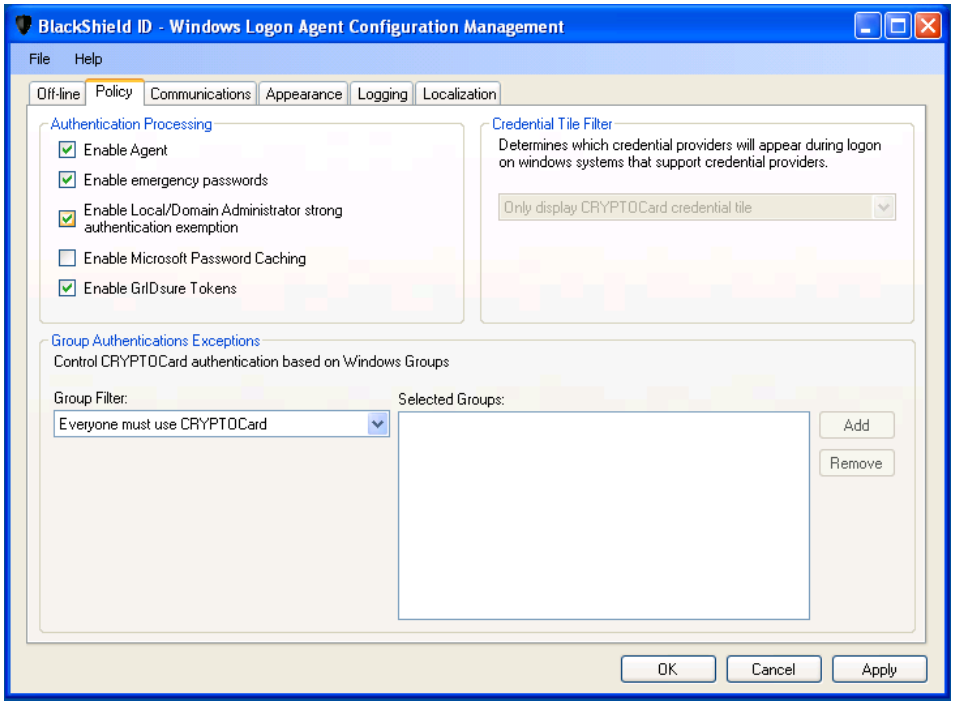


Hanteringen av tilldelningen av inloggningsförfarande kan ske på olika sätt. Antingen tilldelar administratören provisioneringen av inloggningsförfarandet eller så låter man systemet tilldela detta utifrån vilken grupp användaren som synkroniserats in tillhör.

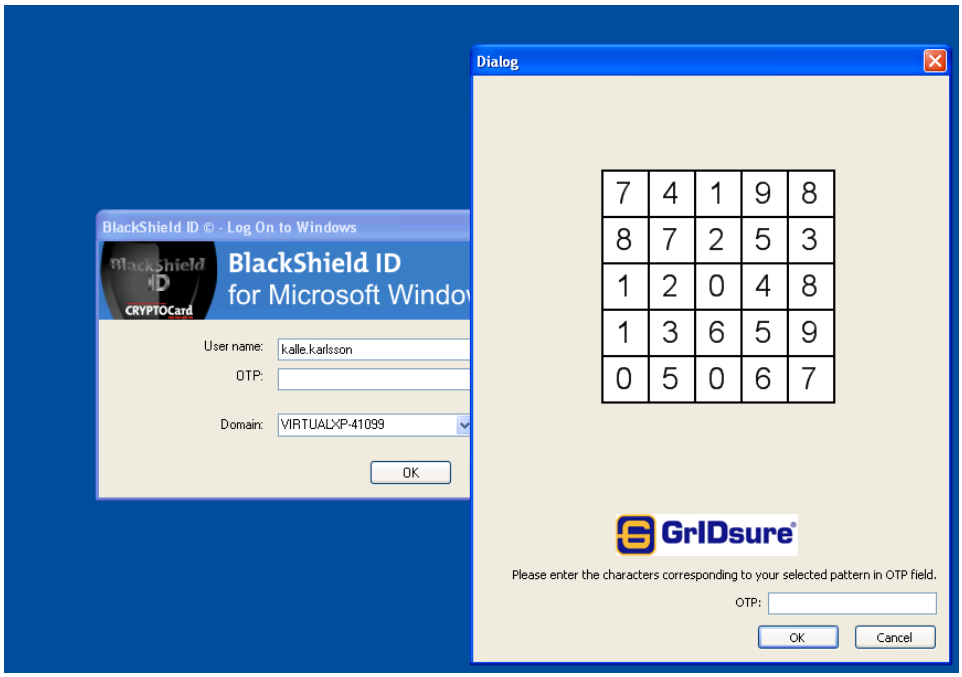
Man kan tilldela flera olika inloggningssätt för en användare, exempelvis både Gridsure och SMS. Om användaren har en epostadress angiven för sin användare skickas det automatiskt ut en kod som användaren ska använda. I ett separat mejl kommer också en konfigureringsfil som användaren importerar i sin inloggningsapp om det är den funktionen avändaren ska ha. Alternativt att användaren skickas till en sida där man får konfigurera sitt konto.



Det finns möjlighet att plocka ut konfiguration för användaren och istället låta användaren få hämta ut det via ett besök hos exempelvis servicedesk.



I Windowsklienten finns det några val att göra där man kan exempelvis kan se till att lokala administratörer och domänadministratörer ska kunna logga in på maskinen utan att använda tvåfaktorsautentisering. Detta är något att rekommendera då man kan ansluta till datorn om något skulle bli fel på mjukvaran.



Exempel på gridsure-inloggning

Inloggning med genererad kod

Skalbarhet

I och med att allting ligger i molnet och det enda som sker lokalt är en mjukvara som pratar med molnet är skalbarheten bra.Skulle man vara rädd för att ha hanteringen i molnet så finns lösningen att sätta upp för lokal installation. Då kan man flytta hela sin konfiguration från molnet till lokal server.

Sammanfattning

Safenets lösning är väldigt smart upplagd och enkel att hantera när man väl hittat igen alla inställningar och gjort den första konfigureringen. Här rekommenderas att man tar hjälp av en konsult med uppsättningen så man får det konfigurerat som man vill ha det då det inte är helt lätt att sätta sig in i alla inställningar om man inte fått en bra genomgång av mjukvaran.

Nackdelen med systemet är att det är ganska stort och komplext. Det innebär att det tar ett tag att komma igång med och sätta upp all konfiguration. Men det är också en fördel att det innehåller stöd för alla möjliga scenarion. Rekommendation är att använda den då man vill stödja flera plattformar. Och få ett brett stöd av autentiseringsmöjligheter.
Denna lösning är dock inte att rekommendera om man vill säkra upp enstaka system.

4.3.2 Mideye

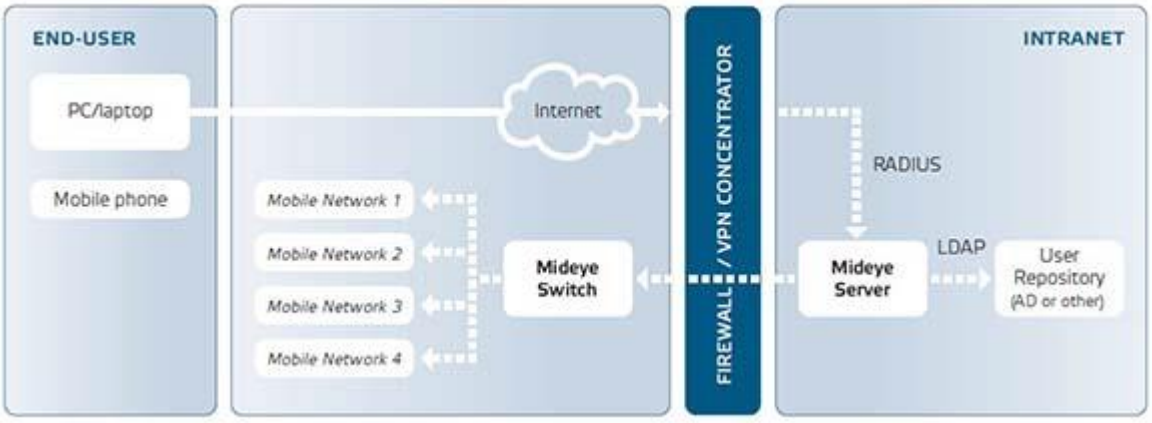
Mideye är svenskutvecklat av en avknoppning från en del av Ericsson.

http://www.mideye.com/index.php

Teknik

Lösningen består i en lokal server som integreras mot en LDAP-katalog för att synkronisera över användare utifrån exempelvis grupptillhörighet.

Vid inloggning genereras en kod på den lokala servern (Mideye server) som kontaktar en tjänst hos Mideye (Mideye switch). Den i sin tur använder sig av lämpligt mobilt nätverk och skickar ett sms till numret som stod angivet på användaren som försökte logga in.



Plattformsstöd/Tjänster:

- Checkpoint VPN and firewall
- Cisco VPN and firewall
- Citrix Access Gateway
- Citrix Web Interface
- Clavister firewall and SSL VPN
- F5 SSL VPN
- Juniper SA SSL VPN
- Linux PAM
- Microsoft Exchange
- Microsoft IIS
- Microsoft Sharepoint
- Microsoft Terminal Services Web Access
- Microsoft Threat Managment Gateway TMG
- Microsoft Unified Access Gateway UAG
- Microsoft Windows Terminal/Remote desktop Services
- Open SSH

- Portwise SSL VPN

Administration/användarhantering
Användare läggs upp i Active Directory och synkas mot tjänsten. Administrationen består i att man lägger upp mobilnummer på användaren. Sedan är det i princip självgående.

Skalbarhet
Vi har ingen egentlig information om hur systemet skalar. Men i och med att administrationen är minimal och allt sker via SMS så ska det inte vara något problem med fler användare.

Sammanfattning
Det man betalar för med Mideye är deras SMS-funktion och att de hanterar den. De håller koll på att SMS levereras korrekt och detta innebär att företaget garanterar att koderna kommer fram till användarna även om mobiltelefonen för tillfället saknar täckning. De använder sig av flera mobilnätverk om det skulle vara problem med flödet på något av näten. Man får fullständiga rapporter över hur det har gått med SMS:en med mera.

För användare som befinner sig utanför nätets täckningsområde finns Mideye+ som är en mobil applikation som möjliggör inloggning även när mobiltelefonen saknar nätåtkomst. Operativsystem som stöds för närvarande: Android och iPhone.

Mideye autentiserings tjänsten stödjer också autentisering med koddosor.
Koddosorna kopplas till användarna genom manuell inmatning.

Det man måste se till att hålla koll på är att man kopplar rätt mobilnummer till rätt användare och hur man säkrar upp detta. Det finns inga lösningar för att hjälpa användare som har tappat bort sin

mobil eller fått slut batterier. På Umeå kommun har man löst det genom att om de kunde verifiera användaren så ställde de om numret i AD:t på användaren och bad användaren försöka logga in så de fick sms:et till sin mobil istället och läste upp koden för användare så de kunde logga in och ställde sedan tillbaka numret.

4.3.3 Authlite v1.2 (v2)

http://www.collectivesoftware.com/solutions/authlite

AuthLites tvåfaktorsautentiseringslösning förstärker Active Directorys normala lösenordssäkerhet med med en enkel knapptryckning på token för varje användare.

Teknik*:*
Authlite installeras på alla Domain controllers i Active Directory.

OTP Token. AuthLite använder Yubikey från Yubico Inc. Yubikeys har ingen display, de drar ström från USB-porten och behandlas som en HID tangentbord enheter så att de fungerar utan särskilda drivrutiner på alla plattformar.

OATH Token. AuthLite är också kompatibel med One time lösenkod som genereras av en smartphone - token app.

Plattformsstöd/Tjänster:
v1.2 (Beta)

- Windows XP
- Windows Vista
- Windows 7
- Windows 2003
- Windows 2008

v2

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 2003
- Windows 2008
- Windows 2012

Administration/användarhantering
Systemets administrationsgränssnitt är enkelt och lätt använt finns även bra stöd i manualer och även filmer för olika ändamål. När det gäller felsökning så finns det mer att önska av produkten.

Skalbarhet
Fristående system med lokala användare
Vid denna tid, kan AuthLite version 2 bara användas på maskiner Domain medlemar.
AuthLite v1.2 kan installeras och användas för fristående servrar / arbetsstationer men har ej stöd för 2012.

Sammanfattning
Authlite är en enkel produkt som kräver lite kunskap för att implementeras i en driftmiljö, Yubikey som används fungerar mycket bra och vissat sig vara mycket hållbar. Att man sedan måste nästan ett år för att få stöd för ett nytt Windows operativ är inte hållbar. Några månader kan man tycka vara en rimligare tid att vänta på ett nytt stöd.

4.3.4 Clavid - Clavid Internet Identity Provider
Contact and Company information

Clavid AG

Business Center St.Gallen
Kornhausstrasse 3, Bahnhofsplatz
CH-9000 St.Gallen
Switzerland

Phone: +41 (0)71 222 54 33

Web-site: http://www.clavid.com

Technology

Clavid provides Authentication as a Service (AaaS) for Web application using common Single-Sign-On (SSO) standards.
Clavid provides a service, not a specific technology or software. No information is given about how the actual service is implemented.

Platform Support / Services:

Clavid currently supports different authentication systems that can be combined for multifactor (1 or 2 FA) user-authentication. In particular:

- User credential [username&password],
- SSL certificate,
- Yubikey (Yubico) [USB token],
- Google Authenticator [mobile applet],
- AGSES cards [Fingerprint protected OTP generator dongle],
- TiQR [mobile applet].
- …

Clavid provides SSO service by common standards for web-application (OpenID, SAML 1.1/2.0), but it also claims support for some kind of proprietary/customized solution. Clavid does not support SSO standards for O.S. or other not web-based services. For example: Windows login (AD or standalone), Linux/Unix, Kerberos, etc… Instead, Clavid expressed some kind of interest into a possible future integration with RADIUS.

Authentication policies can be set for all users, but option can be left for customization. For example it might be possible to allow username/password authentication as well as Google-authenticator and Yubikey. User might decide at each time if authenticate using username/password, or using Yubikey OTP alone, or a two-factor credential + yubikey or credential + Google-Authenticator… The kind of authentication chosen by user might be passed as attribute to the service-provider (SAML attribute or OpenID PAPE extension) leaving to local-service the decision if the chosen option is secureenough. In such a scenario, it is possible that user normally authenticates with a single factorauthentication, but some services will eventually require a re-authentication with a more secure option for granting access.

AaaS Clavid service can be deployed in three different ways:

- (Clavid recommended option): In such a scenario authentication is provide as a “cloud” service,
- Clavid might provide a dedicate system instance installed into costumer’s premises. In such a scenario the costumer is the exclusive consumer of the specific instance, but Clavid keep full and exclusive control/administration of the system,
- Clavid might provide software installation package and support to costumer under license. Such it is actually a “shared administration” scenario similar to previous one, but more control by costumer over its own service-instance. Configuration/maintenance is still strictly controlled by Clavid-support under the term of support-agreement.

Please note Service/Support cost grows when costumer requires local instance and more control on it.

Administration / User Management:

Clavid might use its own Identity-manager for users' verification, but this is not normally requested by costumers. In such a case, a trust-connection is set between the costumer's user-directory system and Clavid authenticator-service. This is normally done for checking if user exist (Username) and verify his/her password. LDAP is largely used for this purpose. When using a second authentication factor, or an hardware token, Clavid might use it's own DB for storing secrets (for example Google Authenticator key) or use a third-party identity-verification-service related to the specific authentication solution. For example: yubikeys use a secret symmetric-key (AES-128), Clavid verify OTP using Yubico authentication system assuming that original secret was not overwritten by costumer. In case, it would be possible to set Clavid authenticator to verify Yobikey OTP (or other kind of second factor secrets) against specific costumer-provided OTP verification service as is done for user/password (LDAP). Note, the software/tools required to set a local second-factor authentication is not always provided by token/solution producer. Ad-hoc solution might be required.

Scalability:

Clavid claims its solution is highly scalable, and it provides support to hundreds of thousands of users. References might be provided since Clavis service has been adopted by different companies and public/government institutions.

Summary:

Clavid authentication-service was reviewed and tested with the direct support and help of Clavid. The company showed interest into this review process and they nicely provided all requested information and explanation. Almost all information reported into this document come from video-conferences and email exchange with Clavid.

For the actual tests, Clavid free service was used. The free service is limited with respect to full-service (only OpenID and only Clavid Identity-Manager can be used), but fully functional with respect to authentication options and main per-user policy configuration. Tests were run using an ad-hoc Clavidfree account and a test OpenID based service-provider (Apache2/Ubuntu and PHP-OpeID library).

Tests could be not extensive and could not cover the key integration issues. The last is actually an important note. Integration (University Identity manager and eventual Keys-DB) is most probably the key challenge for Clavid Authentication deployment. However, tests showed the large flexibility offered by Clavid service and also give the possibility of appreciating the different characteristics of the many supported authentication solutions. In particular: Yubikey, Google-Authenticator and TiQR.

An evaluation of Clavid solution must begin with the fact that **Clavid provides a service**. This obviously means **outsource** the critical authentication service. Key points:

- **Regulation frame:** is it possible to outsource such a critical service? There are two options: use a shared/cloud solution, or deploy a dedicate service-instance. Clavid will anyhow control the system.

- **Service Cost:** Total Cost of Ownership for authentication support must be estimate for a proper evaluation of Clavid's offer.

- **Service Utility:** Clavid service review was positive, but there is a critical limitation. The service provided is relevant and it would allow solving now and at least on short and medium period, many of the critical issues about web-application and cloud-service authentication. For example, it would be possible to allow different institutions, groups, application using the authentication level (1 factor, 2 factors) it better matches their needs. It would also be possible to use different kinds and combination of authentication tokens/solutions. Integration of new coming standards (SSO) or authentication system (token/dongle/App) will not request any further investment into system integration/support, but buying more gadgets. The critical limitation is that Clavid service focus on web-application and cloudservices. In order to provide a complete enhanced authentication including 2FA for all systems (Windows and UNIX based) it is necessary choosing a second, and eventually a third, solution. The overall integration of all parts is an open issue of possible complex solution. Clavid will not solve this problem, but they show interest in helping for their part.

- **Service Warrenty:** no information is available for a correct evaluation of Clavid service warrenty. Service-Level_agreement must be defined and the company/service evaluated in particular for the critical security aspects of this service. Clavid is expected to provide interesting references since its service was adopted by different companies and public/government services.

4.3.5 Microsoft Azure

Azure har inte gått att utvärdera fullt ut men kan vara en intressant produkt I framtiden.
Därför att vi bara valt att presentera produkten med Microsofts egna ord om produkten.

Windows Azure Multi-Factor Authentication

Windows Azure Multi-Factor Authentication är ett extra autentiseringslager utöver användarens kontoinformation, vilket minskar organisationens risk och bidrar till föreskriftsefterlevnad genom att göra personal-, kund- och partneråtkomst säker. Windows Azure Multi-Factor Authentication kan användas med både lokala och molnprogram.

Få säkerhet och bekvämlighet

Windows Azure Multi-Factor Authentication skyddar åtkomsten till dina data och dina program, samtidigt som det fyller användarkraven på en enkel inloggningsprocess. Tjänsten ger förstärkt skydd mot hot från skadlig kod, och varningar i realtid meddelar din IT-avdelning om potentiellt hotad kontoinformation. Multi-Factor Authentication ger stark autentisering via en rad enkla alternativ inklusive mobilappar, telefonsamtal och SMS, så att användare kan välja den metod som de tycker passar bäst. De många metoderna gör att användare alltid kan nås för ytterligare autentisering.

Lägg till det till lokala program

Använd Multi-Factor Authentication-servern till att ge ytterligare autentisering för lokala program som VPN för fjärråtkomst och webbprogram samt molnprogram med Active Directory Federation Services. Synka med Windows Server Active Directory eller en annan LDAP-katalog för att effektivisera användarhanteringen. Kör Multi-Factor Authentication-servern på din befintliga maskinvara eller en virtuell Windows Azure-dator. Flera redundanta servrar kan konfigureras för hög tillgänglighet och redundans.

Aktivera det för Windows Azure Active Directory (Windows Azure AD)

Använd Multi-Factor Authentication till att säkra åtkomst till Windows Azure, Microsoft Online-tjänster som Office 365 och Dynamics CRM Online samt molntjänster från tredje part som integrerar Windows Azure AD. Aktivera Multi-Factor Authentication för Windows Azure AD-identiteter så uppmanas användarna att ställa in ytterligare verifiering nästa gång de loggar in.

Bygg in det i programmen

Ett Software Development Kit (SDK) ger direkt integrering med dina molntjänster. Bygg in metoder från Multi-Factor Authentication för verifiering via telefonsamtal och SMS i ditt programs inloggnings- eller transaktionsprocess och utnyttja programmets befintliga användardatabas.

Sammanfattning
Eftersom vi inte fått en komplett bild hur man på olika sätt skulle kunna applicera detta i en större skalla på lärosättet så kan projektet idag inte rekomendera Azure 2-faktorslösning som en helhetslösning.

Vi vet att Microsoft har stora planer när det gäller 2-faktor men i detta skeda vet vi inte hur, när det kommer att nå ut på marknaden.

4.4 NATIONELLT IMPLEMENTERAD LÖSNING AV TVÅFAKTORSAUTENSISERING OCH SAML2

Tvåfaktorautentisering och SAML2

Nederländerna
I Nederländerna har SURFnet under andra kvartalet 2012 utrett behovet av en autentiseringsmetod som är säkrare än användarnamn/lösenord för studentinformationssystem, administrativa system och forskningssamarbete med känsliga och medicinska data. Man har beslutat sig för att införa en ny tjänst för IdP:er kallad SURFsure. Denna skall underlätta användandet av flerfaktorautentisering då detta är för dyrt och komplicerat för de flesta av IdP:erna. SURFsure skall kombinera den ordinarie lösenordsbaserade inloggningen med en andra faktor. Om man loggat in med två faktorer förmedlas detta till SP:n.

Eftersom Nederländerna redan har en portal (SURFconext) med ett centralt inloggningsställe för högskolorna så blir det enkelt att där lägga till ett system för den andra faktorn. Med en transparent proxy behöver högskolornas IdP:er inte göra någon förändring. Endast de SP som behöver högre autentiseringsnåvå behöver lägga till RequestedAuthnContext i SAML-requesten. SimpleSAMLphp och Shibboleth stödjer authentication contexts.

Registrering
1. Användaren loggar in via sin IdP.
2. Användaren väljer mellan tiqr, SMS-OTP och Yubikey.
3. Användaren autentiserar sig med den valda lösningen. I SMS-fallet får användaren mata in sitt mobilnummer varefter en engångskod skickas via SMS.
4. En aktiveringskod skickas till den e-postadress som IdP:n angett.
5. Efter aktivering visas ett formulär med alla uppgifter om användaren samt en registreringskod. En begäran om registrering skickas samtidigt till den RA som skall användas.
6. Användaren beöker RA:n och visar upp formuläret med registreringskoden samtidentitetskort.
7. RA:n loggar in och matar in registreringskoden. Inloggningen måste ske med en autentiseringsnivå som är minst lika hög som den användaren valt.
8. RA:n kontrollerar användarens identitet.
9. Användaren får autentisera sig med den valda tvåfaktorlösningen.
10. RA:n bekräftar autentiseringen och kopplar den till informationen från IdP:n.

Det finns två typer av RA, de som kan delegera och de som inte kan. Alla händelser måste loggas och sparas lokalt i minst två månader. Loggarna skall inte kunna läsas eller förändras av någon annan än säkerhetspersonal. En kopia av loggarna skall skickas någon annanstans en gång i månaden. Loggarna skall sparas i minst 180 dagar.

Revokering skall kunna ske inom 72 timmar om autentiseringsnycklar kommer på avvägar.

Uppsala universitet
Man har testat en tvåfaktorautentisering med hjälp av en transparent IdP-proxy. Svensk E-identitet stod för tvåfaktorlösningen (Yubikey). I samband med att Svensk e-identitet flyttade Uppsalas tvåfaktortjänst från test till produktion uppstod en hel del problem med bland annat överföring av metadata från SWAMID. Tiden och resurserna räckte inte till för att lösa problemen så projektet avslutades. Man beslutade att i stället avvakta Inkubator-projektet för en federativ tvåfaktorsautentisering.

Ett problem med proxy-IdP:n var att försäkra sig om att attributen från den ordinarie IdP:n inte förvanskats på vägen. Behovet av tvåfaktorinloggning berodde inte på att man ville ha en högre säkerhetsnivå utan att man ville förstärka nuvarande säkerhetsnivå. Man ville förhindra att någon kunde logga in med stulna lösenord.

Ett önskemål vore att man skulle kunna hantera detta i IdP:n. Då skulle man slippa en proxy-IdP. Visserligen kan man ex.vis i simpleSAMLphp välja mellan flera autentiseringsmetoder men det finns inget färdigt sätt att kommunicera den valda autentiseringsmetodens säkerhetsnivå till Service Providern.

Övriga synpunkter
För att det skall vara någon idé med en säkrare inloggning så måste en Service Provider (SP) kunna begära en viss säkerhetsnivå och få reda på vilken nivå den aktuella inloggningen har. Detta verkar inte särskilt vanligt i högskolevärlden. Däremot brukar man klassificera IdP:erna efter vilken säkerhetsnivå de håller. Det verkar inte heller finnas någon färdig lösning för hur detta skall göras utan man får göra en hel del utvecklingsarbete själv.

Även om man nu får till en lösning där man skickar med säkerhetsnivån i SAML2-svaret till SP:n så måste applikationen på SP:n kunna tolka detta. Även här krävs utveckling.

Ett alternativ till att lägga 2FA centralt i en proxy-IdP är att låta de SP som behöver detta använda en central tjänst för ex.vis engångslösenord via SMS. Det finns flera sådana molntjänster men de är ofta utlandsbaserade. Det vore bättre med en inhemsk tjänst. När man senare kommit överens om hur AuthenticationContext skall användas kan man börja fundera på att lägga 2FA centralt.

Authentication Context i SAML 2
Det finns en mängd attribut i urn:oasis:names:tc:SAML:2.0:ac:classes som Kerberos, MobileTwoFactorContract, Password, PasswordProtectedTransport, X509, PGP, SmartCard m.fl. Hur

dessa skall bedömas säkerhetsmässigt är upp till SP:n. Om man dessutom kombinerar flera faktorer som t.ex Password + X509 blir det än mer komplicerat för SP:n att avgöra tillförlitligheten.

Microsoft stödjer ex.vis bara:

- urn:oasis:names:tc:SAML:2.0:ac:classes:Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
- urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
- urn:oasis:names:tc:SAML:2.0:ac:classes:X509
- urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

Vidare funderingar

Vi skulle kunna sätta upp en IdP-proxy som först pratar med vår ordinarie IdP och därefter kompletterar med en andra faktor. Om det verkar fungera så får vi fundera vidare över hur registreringen av användarna skall ske. Sedan skulle man kunna låta ytterligare en högskola testa.

Till att börja med skulle vi kunna använda vår test-IdP + test-CAS + test-Cambro + transparent IdP-proxy. Roland Hedberg, ITS, Umeå universitet, håller på att ta fram en proxy-IdP som vi kanske kan börja testa i slutet av november.

Problemområden

- Kan man ha flera tvåfaktorslösningar eller måste alla användare ha samma? Det kan bli problem för de som redan använder ex.vis Yubikey. Jag tror inte man vill hålla reda på flera manicker.
- Tilliten till den centrala IdP:n. Hur garanterar man att den inte förvanskar informationen mellan högskolans IdP och tjänsteleverantören.
- Skall användarna ha två olika IdP att välja på när dom loggar in, en för 2-faktor och den Sid 4 (4) egna när bara lösenord räcker. Det kan ge upphov till förvirring.
- Hur skall användarna registreras? Användaruppgifterna kommer ju från olika källor: LDAP, Active Directory etc.
- Finns det applikationer (SP) som kan tolka en angiven säkerhetsnivå i SAML-svaret?

5 SAMMANFATTNING

Tittar man idag på dom behov som finns så finns det fördiga produkter som går att nyttja, men kostnaderna är höga och den egna kontrollen blir blir inte lika tydlig som när man jobbar med systemens behörighetssystem (Lokala konton/grupper eller AD). Kostnaden kan man säkert motivera i mindre implementationer men vill man skala ut till en större nyttjande så blir det svårare att räkna hem.

Vi har under projektets gång fått ett antal frågor som kommer tillbaka om och om igen.

Vad ska vi ha 2-faktor till? Här måste varje lärosäte sätta sig ner och gå igenom vad är det faktiska behovet är på lärosätet för att kunna välja en bra lösning eller olika lösningar!

Nivåer på säkerhet? Här måste man också planera för hur säkerhetsnivåerna ska se ut för Systemadministratörer, katalogansvariga, HR data, lärare, användare, mm.
Förslag på olika tänkbara nivåer, detta bör man ta fram för alla tänkbara 2-faktors lösningar:
Exempel.

- Systemadministratör av kritiska system T ex. Ekonomisystem, behörighetssystem, skyddade personuppgifter.
- Ledningspersonal
- Nät administratörer
- Systemadministratör av system (ej kritiska), Databasadministratörer.
- Institionsekreterare, Lärare.
- Övrig personal

Den andra faktorn? Många tycker att mobilen är den självklara valet men hur ser den mobila policyn ut på lärosätet och hur säkrar man upp enheten på ett bra sätt, har alla jobb mobiler svar nej! Här får vi en stor frågeställning till att hantera inför ett 2-faktors införande där mobiler ska användas som den andra faktorn.

Och den största och kanske den viktigast frågan är RA funktionen som man måste lösa själv när man implementerar en 2-faktorslösning? (distrubera 2-faktorn, verifiera användare, revokerings hantering, mm.)
I färdiga lösningar så finns det verktyg för flera delar av dessa men organisationen och policy/regler måste arbetas fram.

Av dom produkter vi har tittat på så när det gäller färdiga färdiga lösningar som går att köra i externt moln eller ett lokalt on premissis så är det SafeNet som har det bästa utbudet. Dom har allt från egna tokens, mobil app till att ha möjligheten att köra hela lösningen on premissis dvs. lokalt på lärosätet. Dom är en stor aktör vilket innebär att dom har goda förutsättningar att finnas kvar på marknaden under lång tid. Det starka samarbetet med Microsoft ger också goda förutsättningar att följa med Microsofts förtsatta utveckling av AD:et, vilket betyder att när Microsoft släpper nya versioner så är inte SafeNet långt efter med stödet för den nya versionen.
Mideye har en mycket bra produkt om man vill nyttja deras SMS tjänst som den andra faktorn.

Dom kan verifiera att SMS ”koden” har kommit fram om inte så kan man ändå få åtkommst via en portal tjänst dom har. Finns även möjlighet att använda en token typ koddosa om man inte har mobilt nät eller internet åtkomst.

Tittar man idag på marknaden och på dom behov som lyfts fram under projekt tiden så så ser vi ingen tydlig produkt som kan skala ut stort (<1000) och samtidigt att inte kostnaderna rusar iväg, det sitter inte i tekniken utan kostnaderna.
Pris exempel på SafeNet. (Obs! dessa priser är bara riktlinjer och inte exakta)

500 anv 75,000kr/år
1000 anv 140,000kr/år

Exempel. På ett UmU införande
UmU 4 359 anställda = 600,000kr/år
ITS 200 anställda = 30,000kr/år
Då ingår ej Token/smartcard/ mm., införande kostnaden, förvaltning, system/drift, support, mm.
Beräkna kostnaderna Token/smartcard mellan 25 – 500kr/st beroende på vad man väljer.

Vi anser att har man planer på att skala ut en 2-faktorslösning på en större del av lärosätet så bör man titta på möjligheten att sätta upp en egen lösning (se under REKOMENDATIONER FÖR FORTSATT ARBETE)

Men söker man en mindre komplet lösning och har ont om tid så rekomenderar vi SafeNet som en mycket bra produkt och leverantör, vill man sedan skala upp till en större miljö så är har man alla möjligheter med SafeNet att upp nå det med deras produkt.

Viktigt att påpeka är att man inte är bunden till att välja en 2-faktors produkt utan att man kan ha flera olika för olika ändamål men färre gör det enklare att använda samma policyer och RA funktion. T ex. Ett produkt för Klient login och ett annat för datanäten.

6 REKOMENDATIONER FÖR FORTSATT ARBETE

Eftersom det inkommit flera synpunkter på att inte göra sig helt beroende av leverantörer och få en bättre kontroll på sin 2-faktors miljö så vill vi rekomendera en 2-faktors pilot under 2014.
En 2-faktorstjänst som kan nyttja befintilligt Windows AD och SSH eller var för sig beroende på behov eller en mixad med en färdig produkt
Tanken är att varje lärosäte ska ansvara och utvekla sin egen lösning och bli ”oberoende” av en leverantör, men dela med sig av kunskap och erfarenhet till övriga lärosäten som är med i piloten.

Viktigt att även titta på vad som händer med den nya versionen av E-legitimation version 2 som ska komma under 2014. ((BankID) till de anställda som behövde säkrare inloggning)
Svensk e-legitimation är en tjänst som bankerna tillhandahåller (Bank-ID) och som kan användas för signering/aut. E-legitimation 2.0 använder sig av SAML.
Det kommer att komma en signeringstjänst där man kan signera dokument med den nya versionen.
Man kan också ansluta lärosätet till "Mina meddelanden" som kan användas för ex.vis antagningsbesked etc. (För närvarande används den bara av Skatteverket.)

6.1 LÖSNINGAR SOM INTE GÅTT VIDARE I PROJEKTET

Dessa lösningar har vi valt att inte gå vidare med på grund av olika anledningar.
T ex. skalbarhet, möjlighet till att köra vissa delar lokalt mm.

Sentrybay - Enterprise SAS Two-Factor Solution

SWIVEL - Swivel Secure

Validation and ID Protection Service (VIP) – Symantec

PointSharp – Mobile Gateway