Salvatore Todaro -
stodaro@unime.it

IDEM MFA -WorkGroup Multi Factor Authentication

Presentazione avanzamento lavori

Salvatore Todaro - stodaro@unime.it

Componenti

1. Salvatore Todaro (UniME) Coordinatore
2. Daniele Albrizio (UniTS) Coordinatore (Dimissionario)
3. Maurizio Festi (UniTN)
4. Marco Malavolti (GARR) - revisore
5. Marco Pirovano (UniBocconi)
6. Giuseppe De Marco (UniCal) – osservatore (fino 01/2021)

- Daniele Albrizio (UniTS)
- Salvatore Todaro (UniME)
- Marco Pirovano (UniBocconi)
- Marco Malavolti (GARR)

- Daniele Albrizio (UniTS)
- Salvatore Todaro (UniME)
- Marco Pirovano (UniBocconi)
- Maurizio Festi (UniTN)

Salvatore Todaro - stodaro@unime.it

Premesse ed Eventi

- Inizio Lavori 01/2020
- Emergenza Covid 19 da 03/2020
  - Estremo aumento della complessità degli scenari operativi IT (massiccio uso di risorse cloud)
  - Priorità Enti – Teledidattica/Smart Working
  - Enorme aumento degli attacchi informatici (phishing, ransomware etc) https://www.poliziadistato.it/articolo/385e6120220066d414895301 https://cert-agid.gov.it/news/campagna-ransomware-fuckunicorn-sfrutta-emergenza-covid-19/
- SolarWinds Breach (12/2020)
  - Lista dei clienti potenzialmente compromessi https://web.archive.org/web/20190714085412/https://www.solarwinds.com/company/customers

Salvatore Todaro -
stodaro@unime.it

Attività da “cacciavite”

PoC soluzioni MFA per IDP SAML

Attività di Analisi e Progetto

Analisi soluzioni MFA :

- Analisi di Total Cost of Ownership (TCO)
- Analisi di Return of Investment (ROI)
- Analisi di Impatto sugli utenti e sui servizi
- Analisi Funzionalità, Requisiti
- Etc

Produzione di strumenti di valutazione parametrizzabile e riutilizzabile dai membri

Salvatore Todaro - stodaro@unime.it

Effetti collaterali positivi

Questo WG IDEM-GARR ha permesso ai componenti di:

1. Arricchire la propria professionalità
2. Vedere aspetti, affrontati da altri, prima ignorati
3. Mettere a sistema esperienza, contatti e competenze
4. Catalizzare processi di collaborazione informale tra enti

Fare Community !!!

Salvatore Todaro -
stodaro@unime.it

PoC - Soluzioni MFA per Identity Provider

Shibboleth + DUO SECURITY

simpleSAMLphp + privacyIDEA AUTHENTICATION SYSTEM

PoC funzionante

Marco Pirovano (UniBocconi),
Daniele Albrizio (UniTS),
Marco Malavolti (GARR)

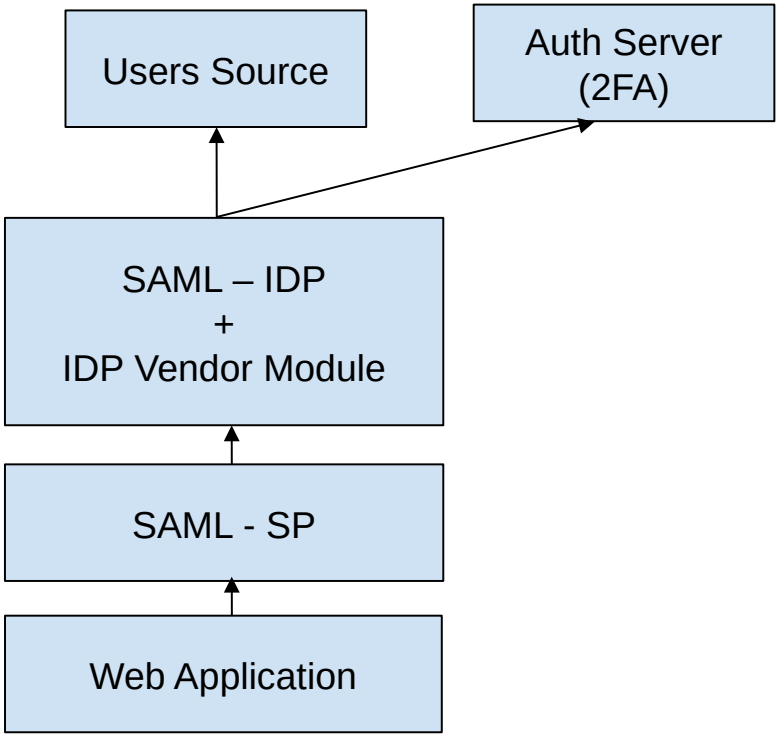
1. Moduli di integrazione esistenti
2. Soluzione in fase di preproduzione da UniBocconi
3. HOWTO in fase di scrittura

PoC (WIP)

Salvatore Todaro (UniME)

Salvatore Todaro -
stodaro@unime.it

Architettura IDP - MFA



Salvatore Todaro - stodaro@unime.it

Questioni Progettuali e di Analisi (tecnologiche)

- Conviene utilizzare MFA solo per le Web Application / Mobile?
- Visti l'impatto sull'utenza è meglio vagliare anche soluzioni infrastrutturali per dare accesso MFA a tutti I servizi/applicazioni/piattaforme ed al determinarsi di eventi?
- Può esistere un secondo fattore univoco per tutte le risorse IT di un Ente, sia esse on-premise o su cloud?

SAML v2.0
Security Assertion Markup Language

Networks

Auth Server (2FA)

Users Source

Applications

Platforms

IDP

Clouds

WEB Applications

Intranet Resources

SAML v2.0
Security Assertion Markup Language

Active Directory

Microsoft Azure

MySQL

VDI

vmware

CITRIX

NUTANIX

FreeRADIUS
The world's most popular RADIUS Server

Google

ORACLE

Windows 10

Open LDAP

aws

mongoDB

paloalto NETWORKS

FORTINET

CISCO

OneDrive

Microsoft SQL Server

eduroam

PostgreSQL

Ci scusiamo per prodotti o produttori mancanti .... ma sono veramente tanti ....

Salvatore Todaro - stodaro@unime.it

Soluzioni MFA - Vendors

FORTINET

SILVERFORT

DUO SECURITY

privacyID3A AUTHENTICATION SYSTEM

Microsoft

okta

freeIPA identity | policy | audit

Salvatore Todaro - stodaro@unime.it

Soluzioni MFA - Vendors

- Affidando i servizi a terzi ci sono alcuni vantaggi ma:
  - NON si azzera il bisogno di HR interne
  - NON si azzera il rischio informatico
  - NON si azzera la responsabilità legale
  - Aumentano i costi (HR interne) in termini di integrazioni con servizi/infrastrutture/piattaforme esistenti
  - Si aumentano i rischi di vendor/platform lock-in
  - Rischio di perdità di competenze interne

Salvatore Todaro - stodaro@unime.it

Soluzioni MFA - Infrastruttura

1. Salvatore Todaro (UniME)
2. Maurizio Festi (UniTN)
3. Daniele Albrizio (UniTS)
4. Marco Pirovano (UniBocconi)

- Analisi dei requisiti, caratteristiche
- Analisi soluzioni vendor (Documentazione e interviste)
- Analisi funzionali e organizzative
- Analisi di costi e sostenibilità
- Primo modello di analisi dei costi (TCO)
- Impostazione modello di valutazione
- Definizione delle macrosezioni valutative
- Analisi interazione infrastrutture e servizi on-premise e Cloud con MFA
- etc

Questioni non tecnologiche

- Quale secondo fattore scegliere
- Costi Diretti e Indiretti
- Utilizzo di soluzioni open o commerciali
- Usabilità e accessibilità
- Problemi legali (es. esistono scenari dove 2FA/MFA è obbligatoria?)
- Chi e su quali applicazioni e in quali circostanze applicare MFA
- Impatto per Help-Desk e utenza
- Modelli licensing

Salvatore Todaro -
stodaro@unime.it

Tipologia di secondo fattore

1 Token (via Smartphone)

Basso costo di startup (HR)
Ragionevole per scenari NON critici
Basso Impatto Organizzativo

2 Token Hardware

Alto costo di startup (HR)
Ragionevole per scenari critici
Alto impatto Organizzativo
Costo di acquisizione del device

Abbiamo escluso sistemi biometrici

Salvatore Todaro - stodaro@unime.it

Deploy Secondo Fattore

Analisi

Deploy Secondo Fattore	Tempo Uomo Stimato (GG)	Costo Personale Implicito dell'Ente	Utenti MFA
Token Smart Phone (Fascia L1 Immediato)	0,12	€ 15,90	500
Token Smart Phone (Fascia L1 Facile)	1,16	€ 159,02	500
Token Smart Phone (Fascia L1 Media)	3,47	€ 477,05	500
Token Smart Phone (Fascia L1 Massima)	5,79	€ 795,08	500
Token Fisico (Fascia L1)	23,15	€ 3.180,31	500

Salvatore Todaro - stodaro@unime.it

Deploy Secondo Fattore

Analisi

Deploy Secondo Fattore (minuti)	0,1	1	3	5	30
Utenti destinatari del Token	5000	5000	5000	5000	5000
Costo per l'ente	€ 159	€ 1.590	€ 4.770	€ 7.950	€ 47.704
Ore Uomo	8,33	83,33	250,00	416	2.500,00
Giorni Uomo	1,16	11,57	34,72	57,87	347,22

Preso in considerazione

Durante la definizione degli obiettivi (01/2020):

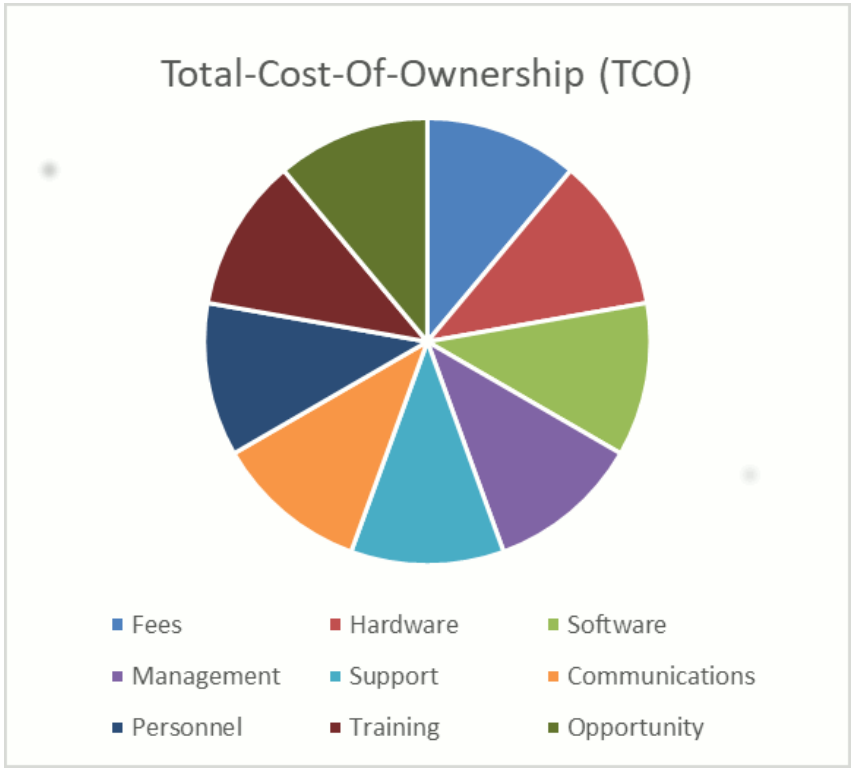
1- Non utilizzabili per tutti i protocolli/servizi

2- Sviluppo necessario di integrazioni

3-Non tutti gli utenti interni potevano ottenere le identità

Salvatore Todaro -
stodaro@unime.it

Analisi dei costi



Salvatore Todaro - stodaro@unime.it

Analisi dei costi

- Costi Vendor (approvvigionamento, manutenzione)
- Costi Personale Interno Help Desk
- Costi Personale Interno per l'integrazione
- Costi Organizzativi (Personale interno impegnato in attività correlate)
- Costi Servizi professionali

Salvatore Todaro - stodaro@unime.it

Risultati inattesi

- Utilizzare software free o open non significa “certamente” avere la soluzione più vantaggiosa per l’ente

- Necessità di esplorare il panorama commerciale per verificare funzionalità integrabilità infrastrutture/Piattaforme/Servizi esistenti

Salvatore Todaro - stodaro@unime.it

Ogni caratteristica ha il suo peso

Macro sezioni

Service & Support	15,00%
Usabilità e Accessibilità	**30,00%**
Funzionalità	25,00%
Costi & Esercizio	10,00%
Log & Auditing	20,00%

Salvatore Todaro - **stodaro@unime.it**

Ogni caratteristica ha il suo peso

Usabilità e Accessibilità		**30,00%**		Valori	Vendor
	Rilascio Secondo Fattore in Modalità Self Service		15,00%	(SI/NO)	SI
	Rilascio Secondo Fattore in Modalità Amministrata		1,00%	(SI/NO)	SI
	Reset Secondo Fattore in Modalità Self Service		15,00%	(SI/NO)	SI
	Reset Secondo Fattore in Modalità Amministrata		1,00%	(SI/NO)	SI
	Attivazione secondo fattore all'utilizzo di un nuovo device		5,00%	(SI/NO)	SI

Salvatore Todaro - stodaro@unime.it

Caratteristiche inserite

Schedate più di un centinaio di caratteristiche ottenute da:

- Analisi in essere presso gli enti
- Analisi dei prodotti presi in considerazione

Salvatore Todaro - stodaro@unime.it

Costi (non solo acquisti)

- Costi di acquisizione
- Costi di avviamento
  (distribuzione del token, integrazione, manutenzione, supporto e formazione)
- Personale interno in fase di esercizio
- Eventuali costi per l'erogazione del/dei secondo/i fattore/i (es. SMS)

Salvatore Todaro - stodaro@unime.it

Risultati ottenuti

- PoC IDP con MFA Shibboleth Duo Security
- Definizione Modello Analitico Comparativo Parametrico
- Analisi dei Costi (diretti e indiretti) delle soluzioni scelte
- Condivisione delle conoscenze ed esigenze presenti e future

Salvatore Todaro - stodaro@unime.it

TODO

- Analisi di Funzionalità (richieste o desiderate)
- Aprire percorsi per acquisti condivisi (es. convenzioni CRUI)
- Valutazione comparativa globale delle soluzioni
- Completamento Total Cost of Ownership (TCO)
- Analisi Return of Investment (ROI)
- Completamento ed evoluzione modello analitico valutativo

Salvatore Todaro - stodaro@unime.it

Per i membri IDEM GARR

- Suggerimenti e collaborazione
- Invito a condividere esperienze / esigenze / visioni

WE WANT YOU!

Salvatore Todaro - stodaro@unime.it

Grazie per l'attenzione.
Domande?