AEC
DATA SECURITY

Autentizace webových aplikací z pohledu NEbezpečnosti.

Oldřich Válka
Security 2010
17.02.2010

LOGIN to APP - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda

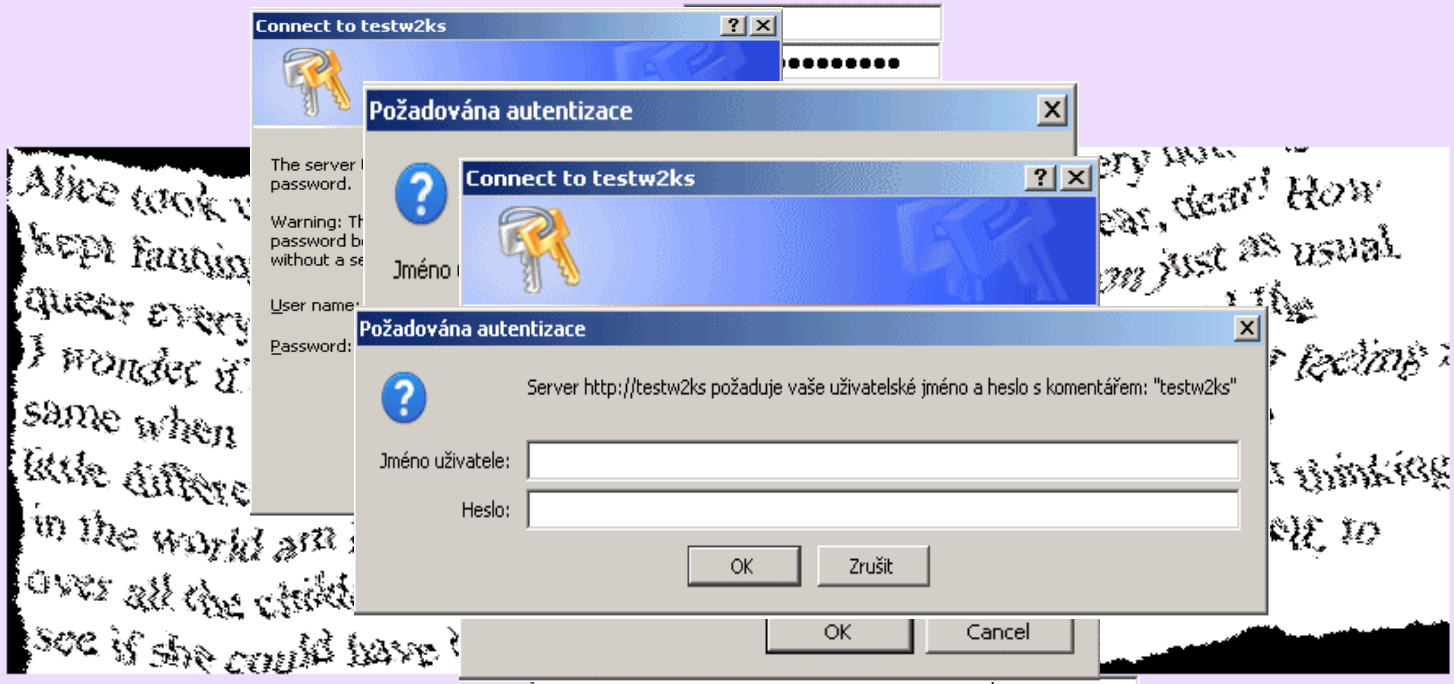
https://somewhere.there/

Google

LOGIN to APP

LOGIN to APP

LOGIN TO APPLICATION



Alice took up the fan and gloves

OPIŠ OBRÁZEK:

Hotovo

Proxy: Nic

Úvod - základní typy autentizací.

- Basic
- Digest
- NTLM
- Formulářová
- Autentizace pomocí Certifikátu
- Autentizace pomocí Apletů
- Další možnosti autentizace

- Jak si vybrat?

AEC
DATA SECURITY

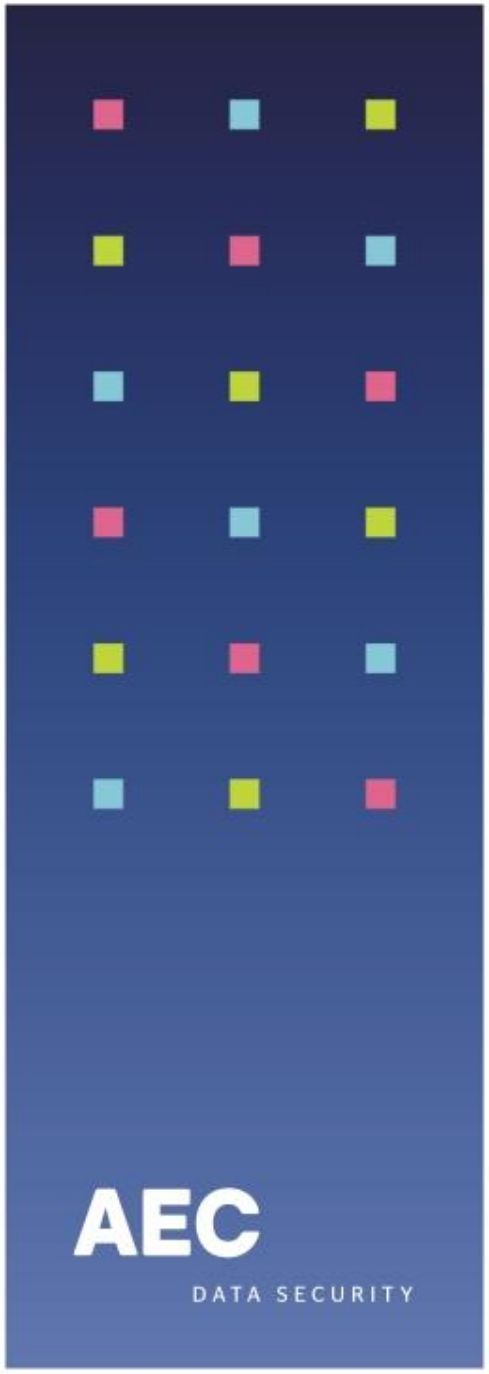
Autentizace Basic - základní funkčnost

- Nejjednodušším autentizace.
- Autentizace pouze zakódována Base 64.

Authorization: Basic
VXppdmF0ZWw6aGVzbG8

=

Uživatel:heslo



Autentizace Basic - základní funkčnost

GET /page.html HTTP/1.1

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="192.168.0.8"

Authorization: Basic VXppdmF0ZWw6aGVzbG8

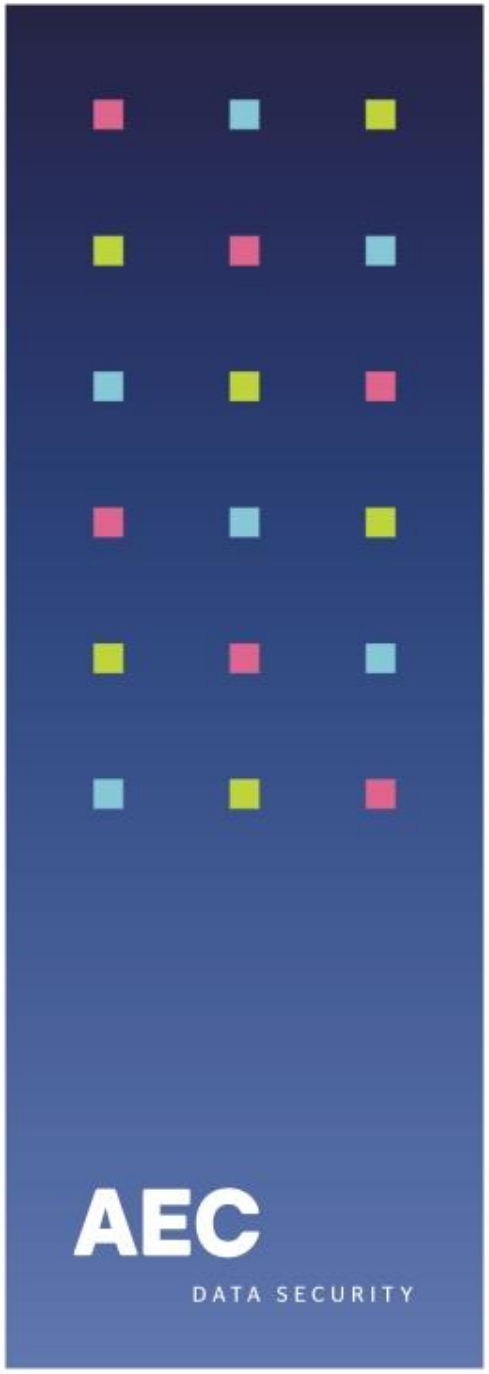
HTTP/1.1 200 OK

	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Autentizace Digest - základní funkčnost

Je bezpečnější variantou metody BASIC.

- Model challenge-response.
- Využívá se hašovací funkce např. MD5.
- Využívá nonce pro znesnadnění zpětné kryptoanalýzy.



Autentizace Digest - základní funkčnost

GET /page.html HTTP/1.1

HTTP/1.1 401 Unauthorized
WWW-Authenticate:
Digest qop="auth",
algorithm=MD5-sess,
nonce="dcd89b7172bc…",
charset=utf-8,
realm="myRealm"

GET /page.html HTTP/1.1
Authorization: Digest
username="test"
realm="myRealm"
nonce="dcd89b7172bc…"
response="6689bc783a…"
…

HTTP/1.1 200 OK

	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Autentizace NTLM - základní funkčnost

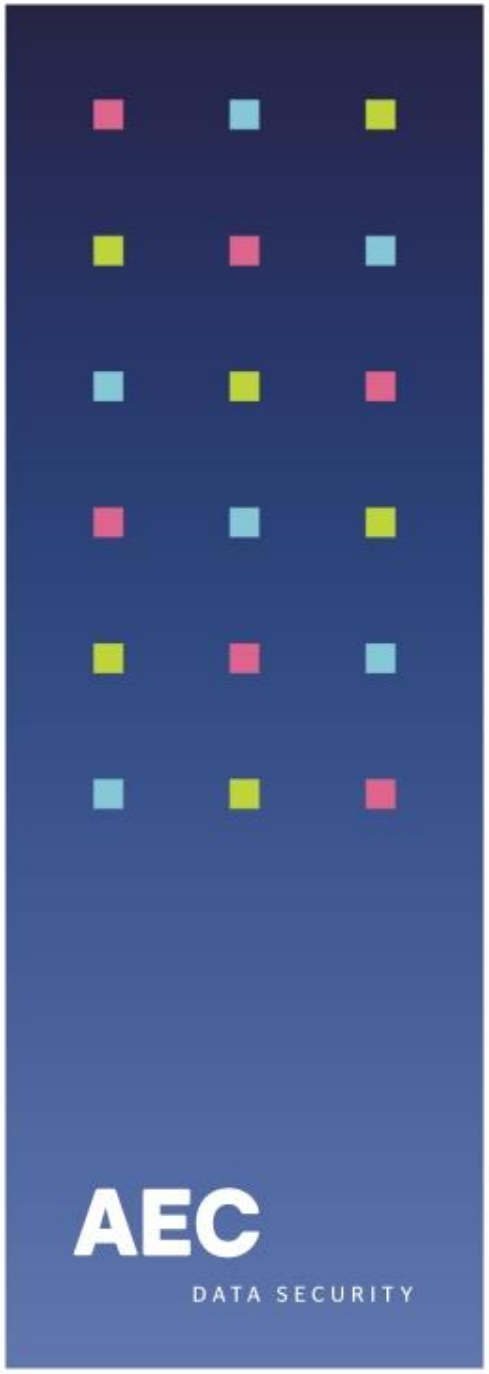
NTLM autentizace:

- Modelu challenge-response.
- Obdoba Digest, vyšší bezpečnost.
- Po celou dobu autentizace musí být spojení otevřeno, jinak se musí proces opakovat.
- Protokol HTTP/1.1 Connection: Keep-alive.

TYPE1 message. Jde o sérii flagu indikujících autentizační možnosti, které klient podporuje. Zakódováno B64.

TYPE2 message (opět 401), který dokončí vyjednávání o nastaveních a vrací klientovi NONCE. Server's NTLM chalenge.

TYPE3 message a dokončí autentizaci pomocí zaHashovaného hesla. Odpověď obsahuje doménu, uživatele, hosta, Lanmanager-response, Nt-Response.



Autentizace NTLM - základní funkčnost

GET /page.html HTTP/1.1

HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM

GET /page.html HTTP/1.1
Authorization: NTLM <base64-encoded type-1-message>

HTTP/1.1 401 Unauthorized
WWW-Authenticate: NTLM <base64-encoded type-2-message>

GET /page.html HTTP/1.1
Authorization : NTLM <base64-encoded type-3-message>

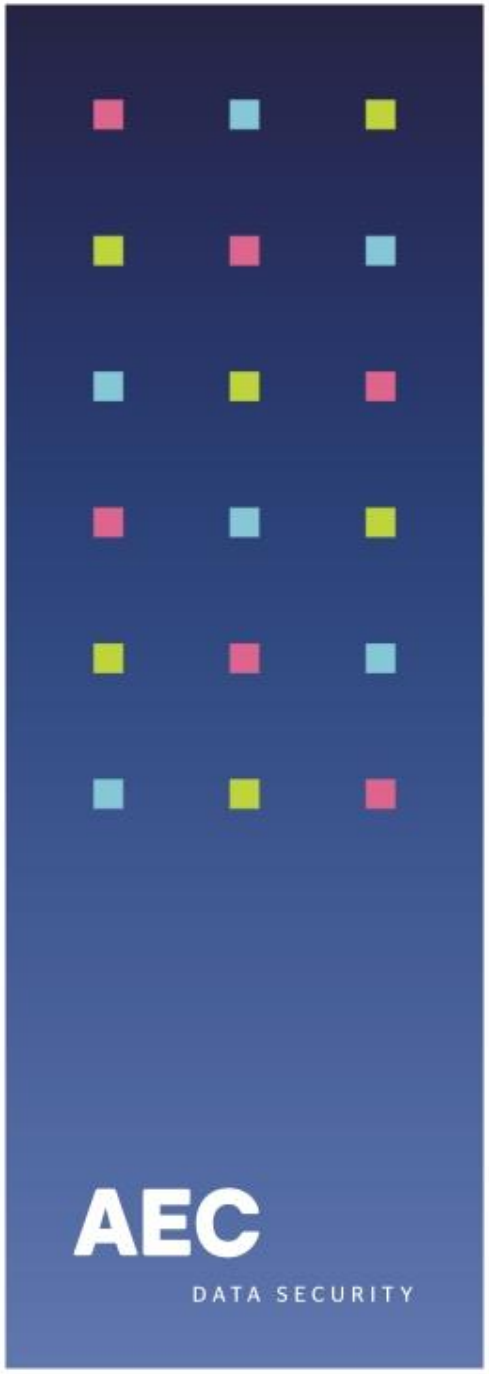
HTTP/1.1 200 OK

	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Autentizace Form - základní funkčnost

Obrovské možnosti. Vše plně v režii vývojářů.

Princip fungování může být od jednoduchého, kdy jsou odeslány autentizační údaje v plain textu až po složité, které šifrují, generují speciální URL, hidden items, různá přesměrování před a po autentizaci atd.



Autentizace Form - základní funkčnost

GET /login.html HTTP/1.0

HTTP/1.1 200 OK

POST /login.html HTTP/1.0

user=test&pass=0293babe7c6e77eb

HTTP/1.0 302
Location: somewhere.else.net/page,html
Set-Cookie: sessionID=1234;path=/;domain=aec.cz;secure

GET https://somewhere.else.net/page.html HTTP/1.0
Cookie: sessionID=1234

HTTP/1.1 200 OK

	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Ukázka

AEC
DATA SECURITY

Autentizace pomocí JAVA nebo ActiveX apletů.

Zde již se vlastně nejedná až tak o tenkého klienta. Applet se ve skutečnosti chová již jako tlustý klient.

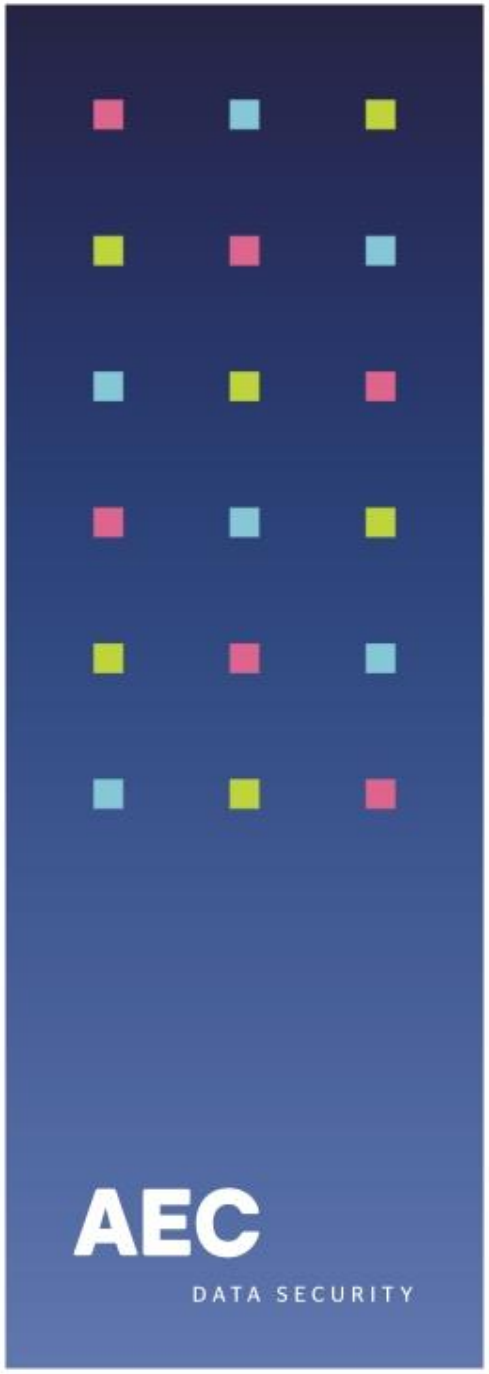
- Možnosti stejné jako Form.

Výhody:

- Možno implementovat všechny možné typy šifrování a ochrany. I asymetrickou kryptografii. Podepisování předávaných dat atd.

Nevýhody :

- Již přílišná robustnost, uživatel se již není schopen přihlásit odkudkoliv.
- Instalace ActiveX, java runtime.
- Ztráta nezávislosti v přístupu odkudkoliv.



	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Autentizace pomocí asymetrické kryptografie.

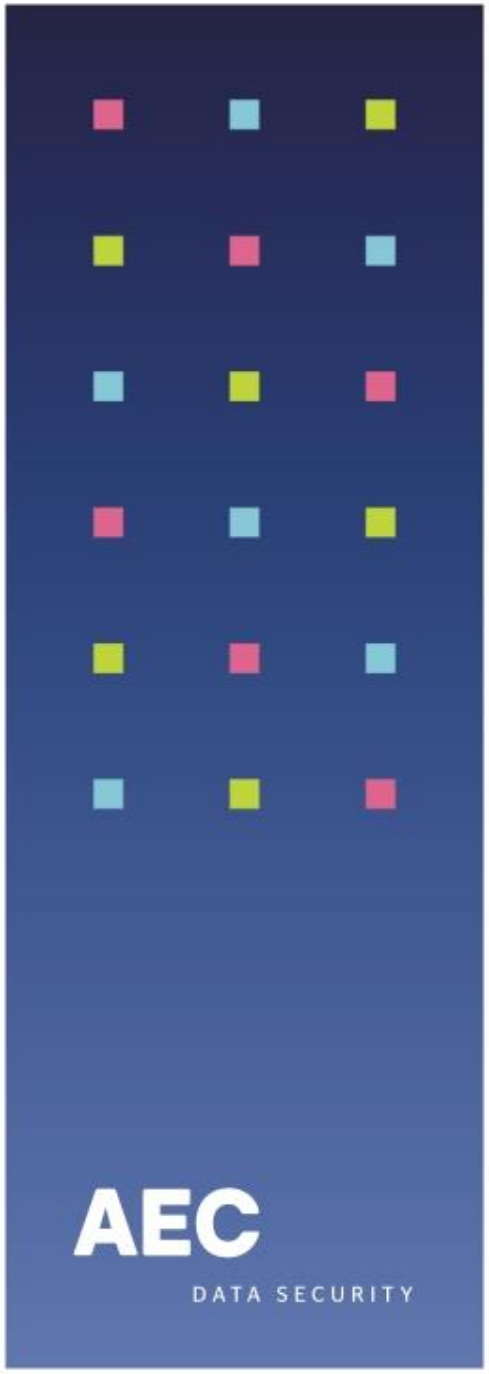
Klientský certifikát může být předáván pomocí prohlížeče případně pomocí apletů.

Výhody:

- Pokud dobře implementováno velmi silná ochrana proti útokům.
- Cracking téměř nemožný.
- Možnost podepisování, timestampovaní aktivních akcí, transakcí.

Nevýhody:

- Pro mnoho lidí špatně srozumitelné a složité.
- Nutnost certifikační autority a PKI.



	Basic	Digest	NTLM	Form	Applet	Cert
XSS	no	no	no	possible	possible	no
SQL Injection	no	no	no	possible	possible	no
Tools avalibility	yes	yes	yes	few	no	no
Cracking - protection	no	no	no	possible	possible	no
Cracking - speed.	1	2	3	1-4	1-4	2-4
Account Protection	no	no	no	possible	possible	-
Nonce (salt)	no	yes	yes	possible	possible	-
Password - transfer	plain	hash	hash	plain/hash	plain/hash	-
Password – saved	plain	plain	hash	plain/hash	plain/hash	-
Challenge - response	no	yes	yes	possible	possible	-

Další typy autentizací

- MultiFactor
- MultiLayer
- OpenID (sso)

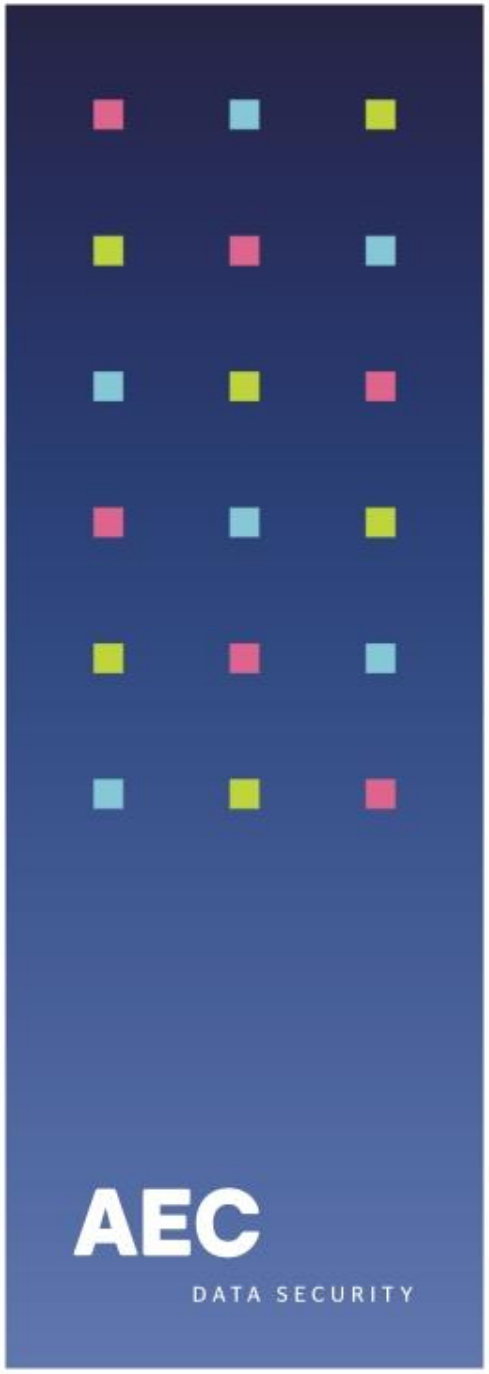
AEC
DATA SECURITY

MultiFactor Authentication

Autentizace se vždy skládá z více faktorů.

Např.

- **Něco co uživatel zná:** heslo, pin ...
- **Něco co uživatel vlastní:** security token, smartcard, mobil, pager...
- **Něco co může mít pouze vlastník:** otisk prstu, rozpoznání tváře, hlasu nebo oční duhovky...



Strong authentication (MultiLayer)

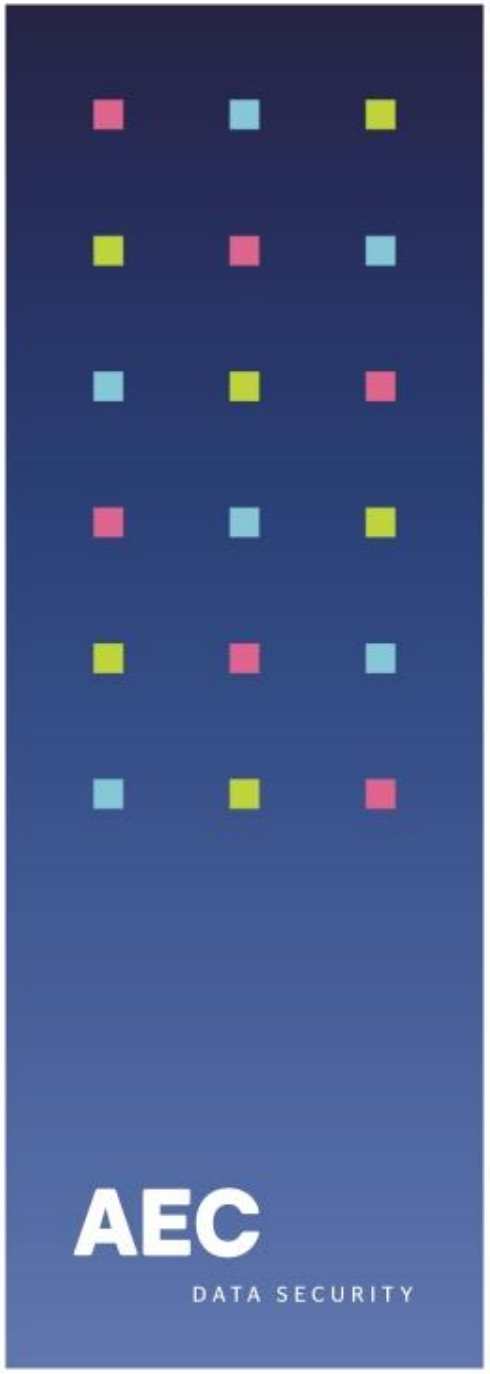
Zde se mluví o MutiLayer nebo MultiTier

Je to vlastně vícevrstvá autentizace. Autentizace spoléhá na dvě a více autentizačních metod.

Například:

- Certifikát (pin) + autentizační údaje.
- Autentizační údaje + OTP.
- Biometrické znaky + autentizační údaje.
- …

OTP (one-time-password) - SMS, e-mail, autentizační kalkulátory, GRIDkarty atd.



Další možnosti autentizace - OpenID.

Independent Authentication Authority (IAA)

Live ID - Microsoft.com
OpenID - openID.net
OpenAuth - aol.com

Výhody:

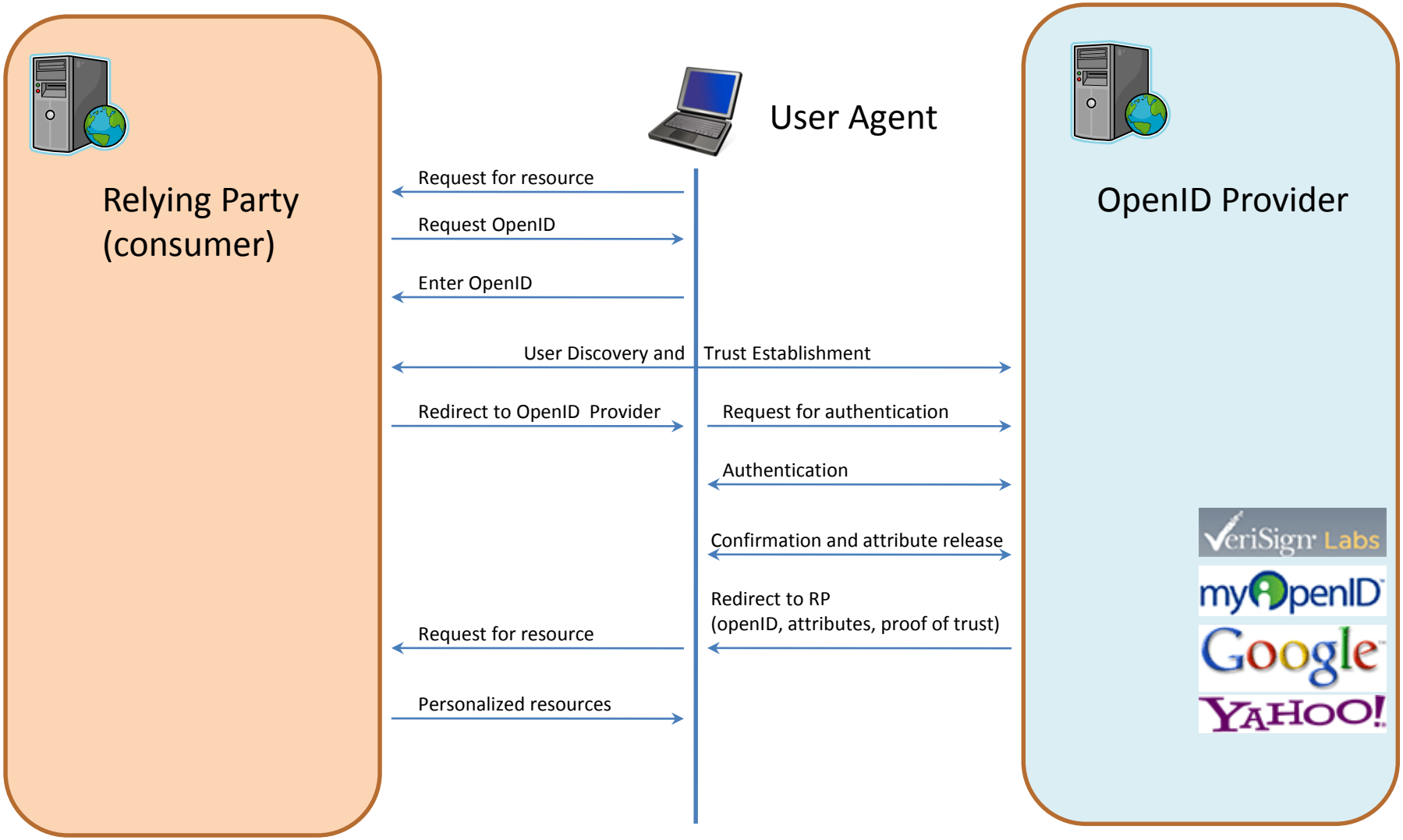
- Uživatel nepotřebuje heslo ke každé webové službě, portálu. Pouze autentizační údaje k IAA.
- Provozovatel webové služby pouze implementuje komunikační rozhraní s IAA. Nemusí se starat o hesla.

Nevýhody:

- Pokud je kompromitován uživatelův účet na IAA získá útočník přístup ke všem aplikacím.
- Bezpečnost spoléhá na cizí mnohdy neověřený element.
- Výpadek komunikace či serveru IAA znepřístupní i vaše aplikace, pokud spoléhají pouze na IAA.

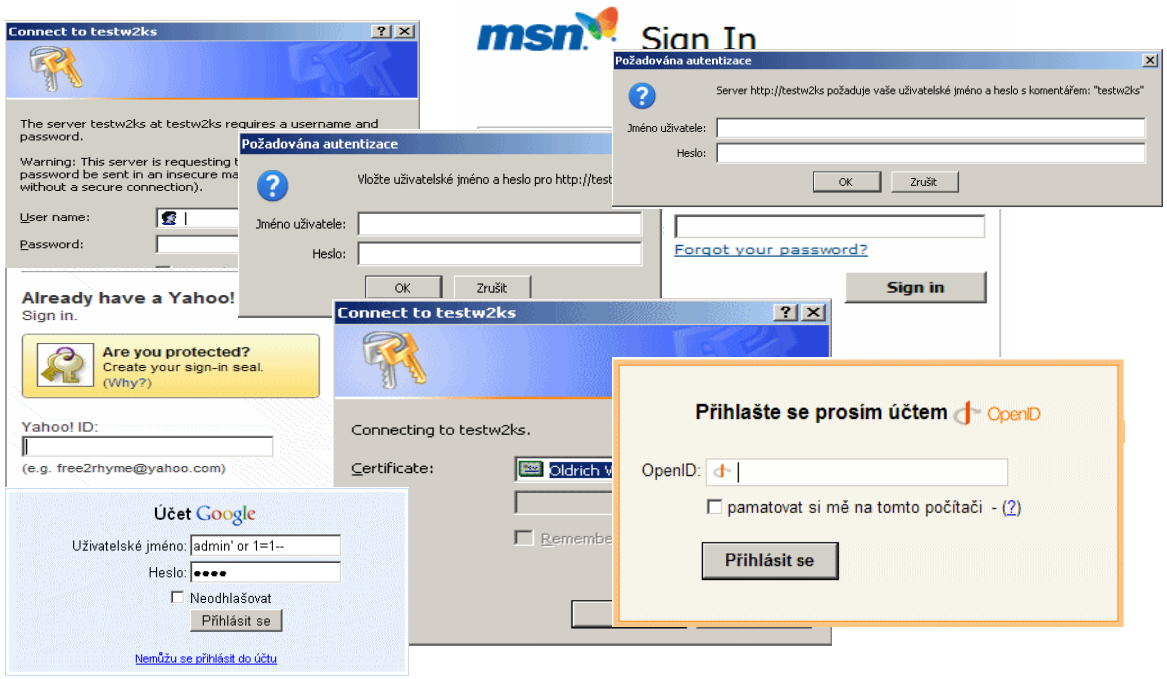
AEC
DATA SECURITY

Další možnosti autentizace - OpenID.



Závěr shrnutí – jak si vybrat?

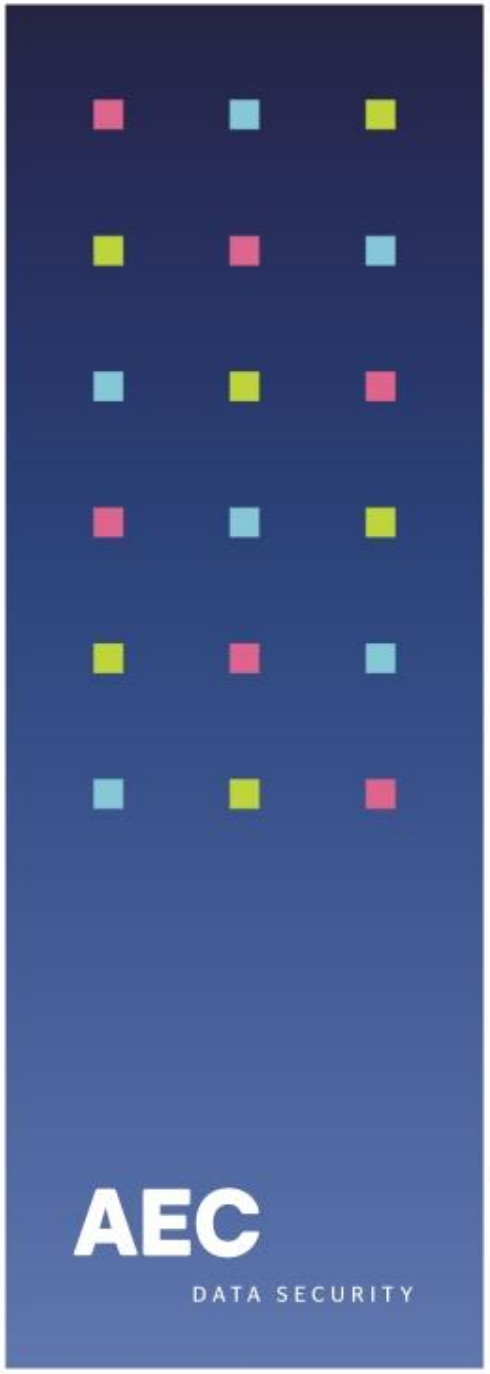
- Nevýznamná aplikace – nízká bezpečnost
- Významná aplikace – střední bezpečnost
- Kritická aplikace – vysoká bezpečnost



AEC
DATA SECURITY

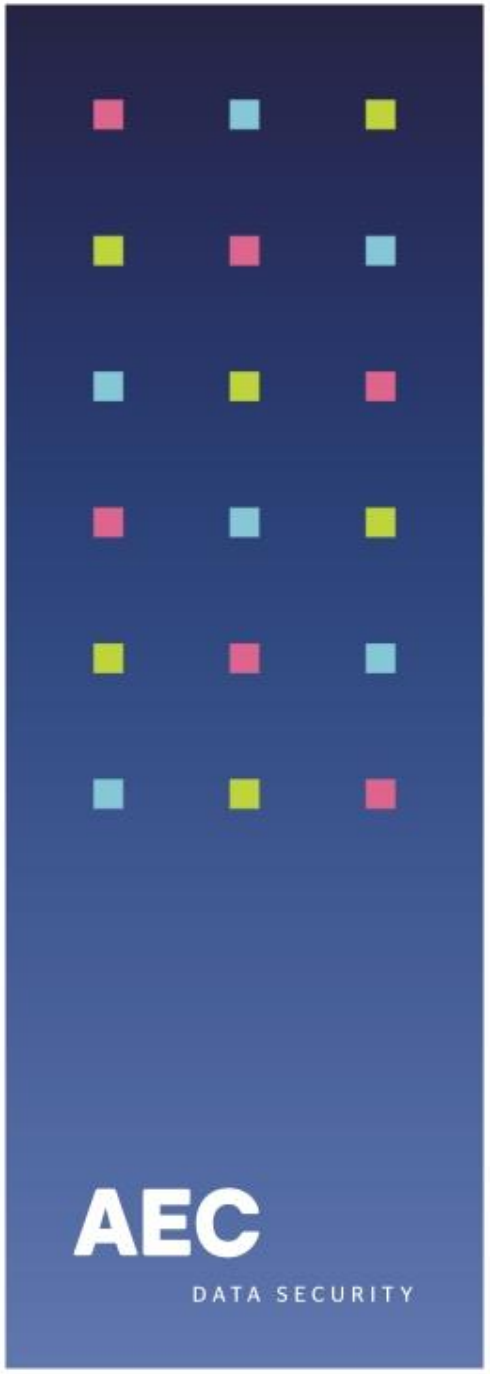
Nevýznamná aplikace – nízká bezpečnost

- Využívat formulářovou autentizaci přes HTTPS.
- Uživatel se hlásí pouze pomocí účtu a hesla.
- Po 3-5 neplatných pokusech je uživatel vyzván k zadání učtu, hesla a captcha.
- V případě dalších 3-5 neplatných pokusů je účet na určitou dobu zablokován.
- Případně je blokována IP, ze které byly neplatné pokusy o přihlášení zaslány.
- Univerzální chybové hlášení. Stejné pro neexistující účet i špatné heslo.
- Implementace politiky hesel.
- Autentizace vždy přes šifrovaný protokol https.



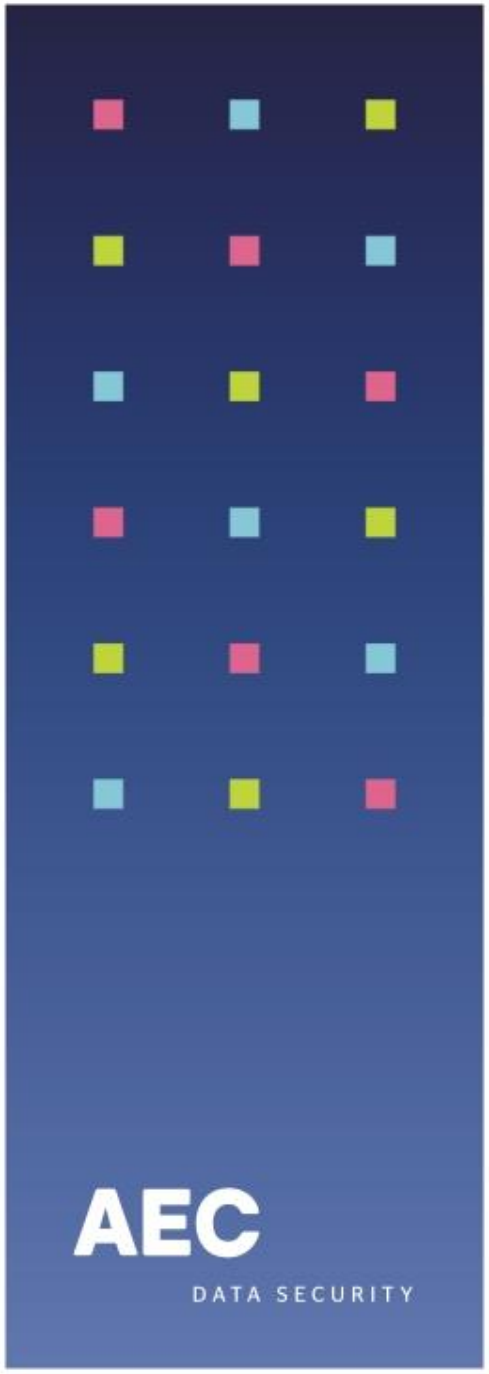
Významná aplikace – střední bezpečnost

- Využívat formulářovou autentizaci.
- Vyžadována MultiFactor a MultiLayer autentizace:
  - Vyžadován uživatelský certifikát pro preautentizaci, ten je uložen (neexportovatelný) na souborovém systému.
  - Implementace OTP.
- Uživatel se dále přihlašuje pomocí účtu a hesla.
- Po 3-5 neplatných pokusech je uživatel vyzván k zadání učtu, hesla a captcha.
- V případě dalších 3-5 neplatných pokusů je účet na určitou dobu zablokován.
- Případně je blokována IP, ze které byly neplatné pokusy o přihlášení zaslány.
- Univerzální chybové hlášení. Stejné pro neexistující účet i špatné heslo.
- Implementace politiky hesel.
- Autentizace vždy přes šifrovaný protokol https.



Kritická aplikace – vysoká bezpečnost

- Využívat formulářovou autentizaci.
- Vyžadována MultiFactor a MultiLayer autentizace:
  - Vyžadován uživatelský certifikát pro preautentizaci, ten je uložen na USB tokenu, smartCard atd. Vyžaduje PIN.
- Uživatel se dále může přihlašovat pomocí účtu a hesla.
- Po 3-5 neplatných pokusech je uživatel vyzván k zadání učtu, hesla a captcha.
- V případě dalších 3-5 neplatných pokusů je účet na určitou dobu zablokován.
- Případně je blokována IP, ze které byly neplatné pokusy o přihlášení zaslány.
- Univerzální chybové hlášení. Stejné pro neexistující účet i špatné heslo.
- Implementace politiky hesel.
- Autentizace vždy přes šifrovaný protokol https.



AEC
DATA SECURITY

Děkuji za pozornost!

- prostor pro otázky -

AEC

DATA SECURITY

Oldřich Válka
oldrich.valka@aec.cz

AEC, spol. s r.o. · Spielberk Office Centre
Holandská 878/2 · 639 00 Brno · Czech Republic
Phone: +420 541 235 466 · Fax: +420 541 235 038

AEC, spol. s r.o. · European Business Center
Dukelských hrdinů 34 · 170 00 Praha 7 · Czech Republic
Phone: +420 267 311 402 · Fax: +420 266 177 155

www.aec.cz