

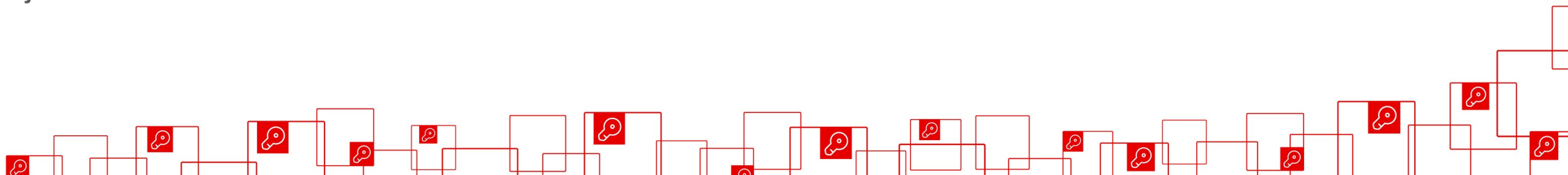


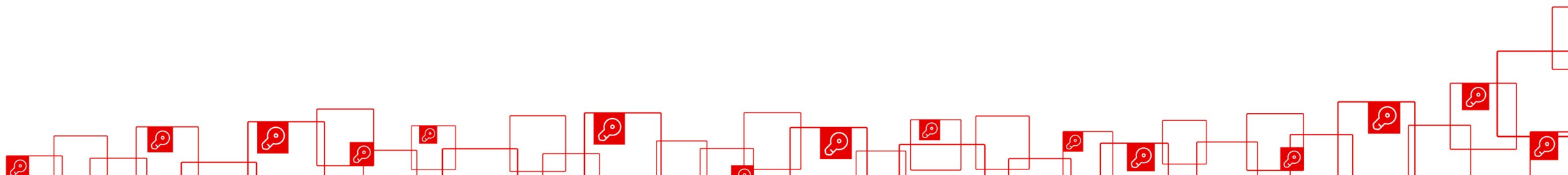
Současný svět certifikátů

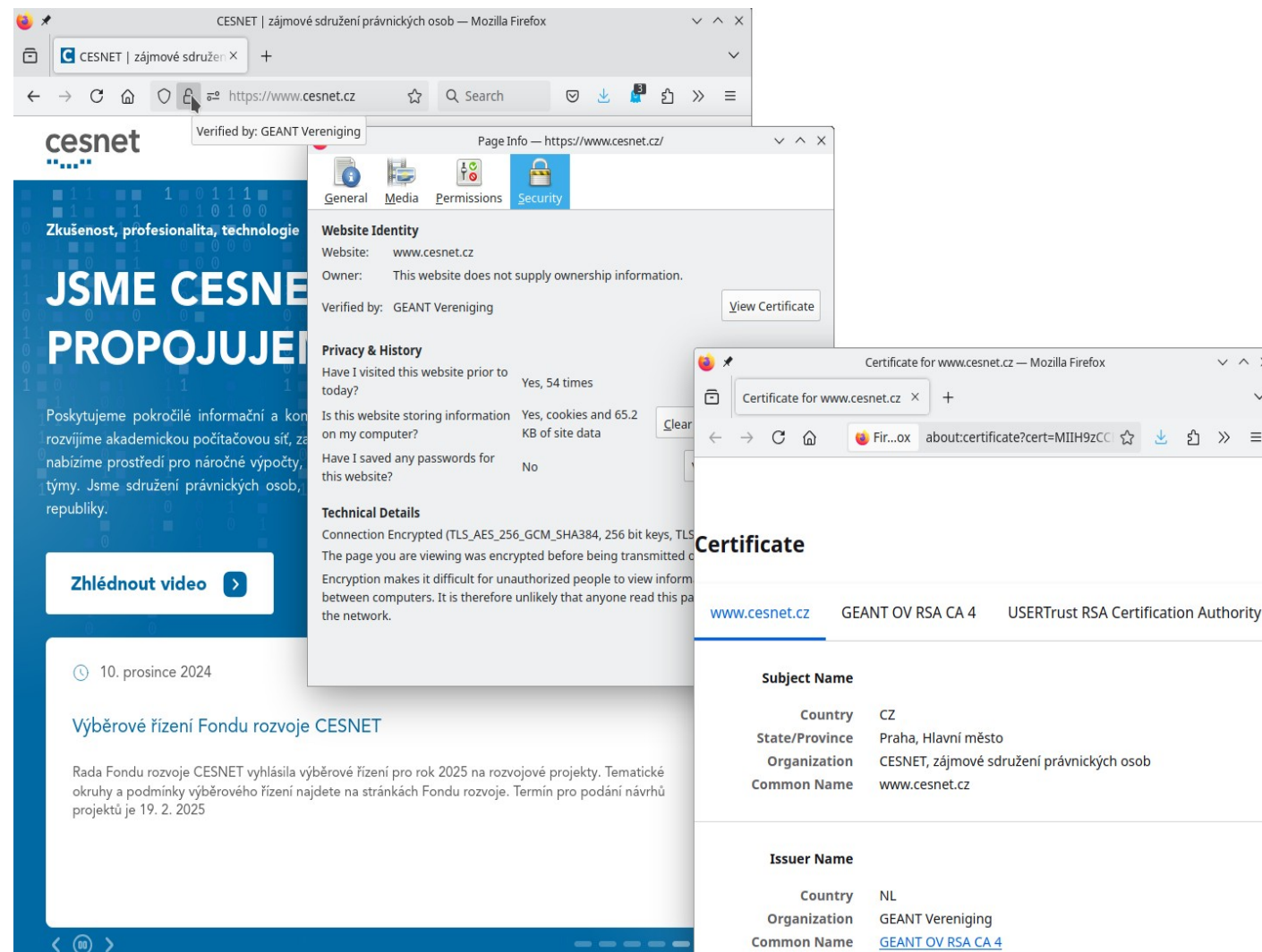
Daniel Studený

Konference e-infrastruktury CESNET 2026

1. října 2026







The screenshot displays a Mozilla Firefox browser window with the CESNET website. The address bar shows the URL `https://www.cesnet.cz`. The website's main content includes the text "JSME CESNET PROPOJUJEME" and a button labeled "Zhlédnout video".

Overlaid on the website is the "Page Info" window, which provides details about the page's security and privacy. The "Security" tab is active, showing the "Website Identity" section with the following information:

- Website: `www.cesnet.cz`
- Owner: This website does not supply ownership information.
- Verified by: GEANT Vereniging

The "Privacy & History" section indicates that the user has visited the website 54 times and that the website stores information on the computer, including cookies and 65.2 KB of site data.

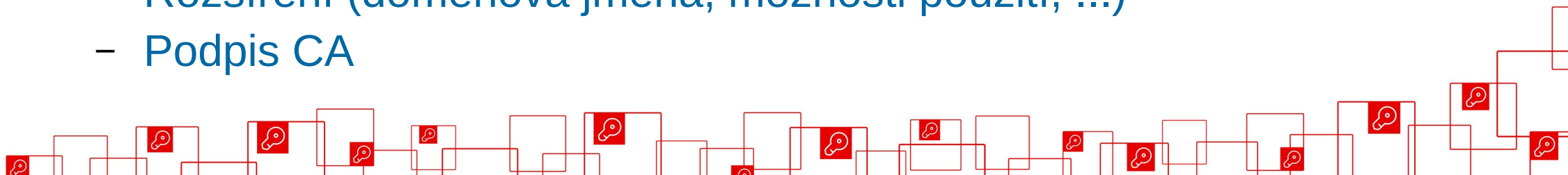
The "Technical Details" section states that the connection is encrypted using TLS_AES_256_GCM_SHA384, 256 bit keys, and TLS. It also mentions that the page was encrypted before being transmitted over the network.

Below the "Page Info" window, the "Certificate" window is open, displaying the X.509 certificate for `www.cesnet.cz`. The certificate is issued by the GEANT OV RSA CA 4, which is part of the USERTrust RSA Certification Authority. The certificate details are as follows:

Certificate	
<code>www.cesnet.cz</code> GEANT OV RSA CA 4 USERTrust RSA Certification Authority	
Subject Name	
Country	CZ
State/Province	Praha, Hlavní město
Organization	CESNET, zájmové sdružení právnických osob
Common Name	<code>www.cesnet.cz</code>
Issuer Name	
Country	NL
Organization	GEANT Vereniging
Common Name	<code>GEANT OV RSA CA 4</code>

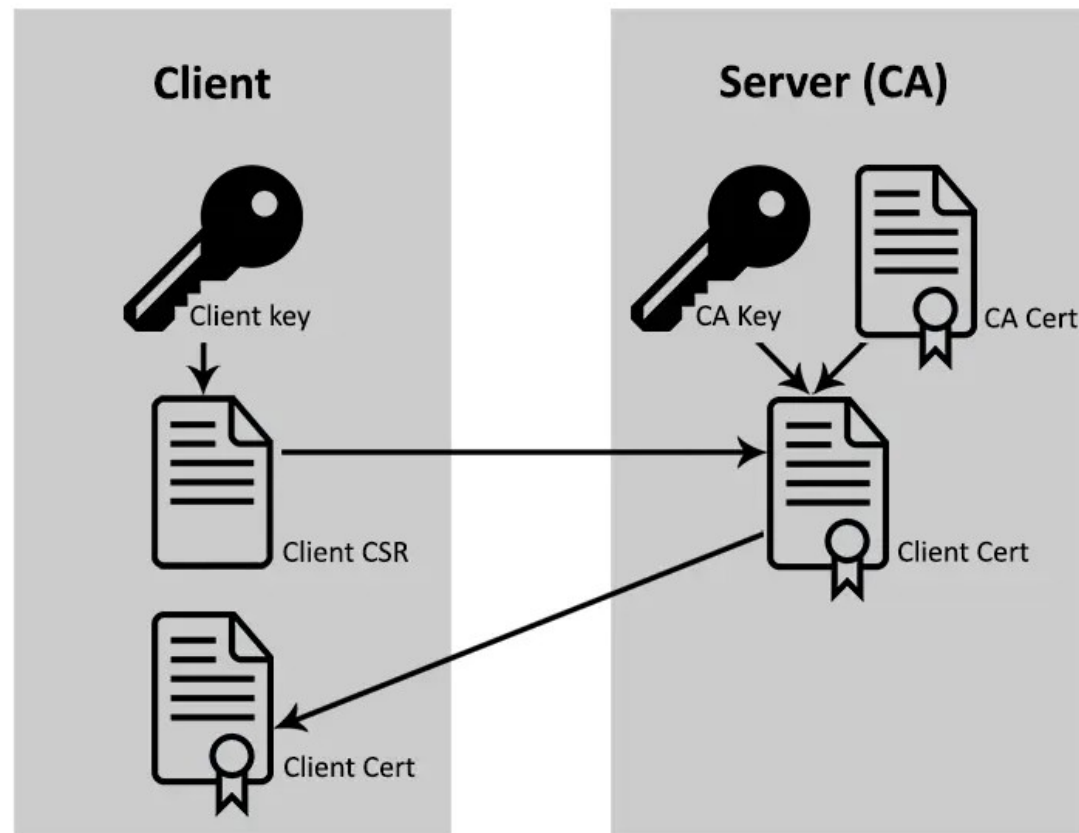


- Standard infrastruktury veřejných klíčů (PKI)
- Autentizace uživatelů, zařízení, programů
- Elektronické podepisování
 - Dokumentů
 - e-mailů (S/MIME)
- Obsah
 - Veřejný klíč
 - Metadata (předmět, CA, platnost, sériové číslo)
 - Rozšíření (doménová jména, možnosti použití, ...)
 - Podpis CA



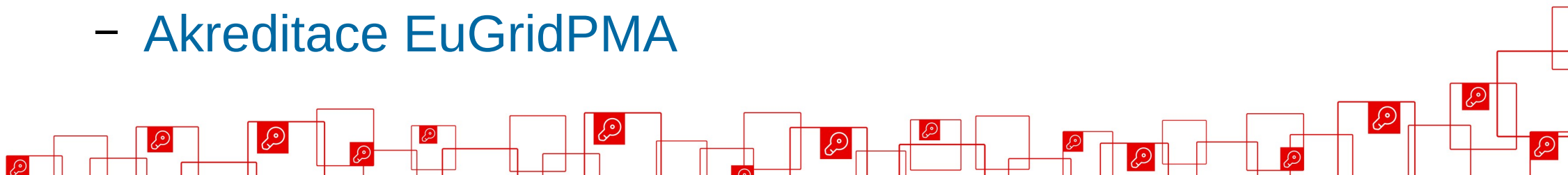


- Využití certifikátů
 - Pro CA
 - Serverové
 - Osobní a robotové
 - Dokumentové
 - Pro podpis kódu
- Certifikační authority
 - Důvěryhodné
 - Kvalifikované
 - Interní
- Typy ověření
 - DV, OV, EV



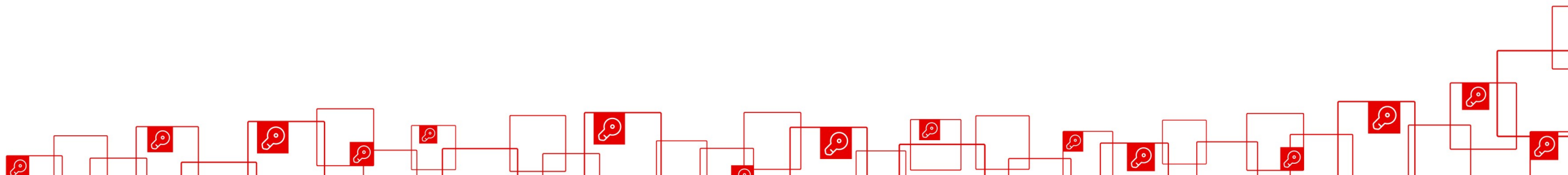


- TEN 155 CZ
 - 2000 - 2003
- CESNET CA
 - 2001
 - Nyní CESNET CA5 (2025 – 2043)
- Certifikáty CESNET CA
 - Distribuované výpočty
 - Akreditace EuGridPMA



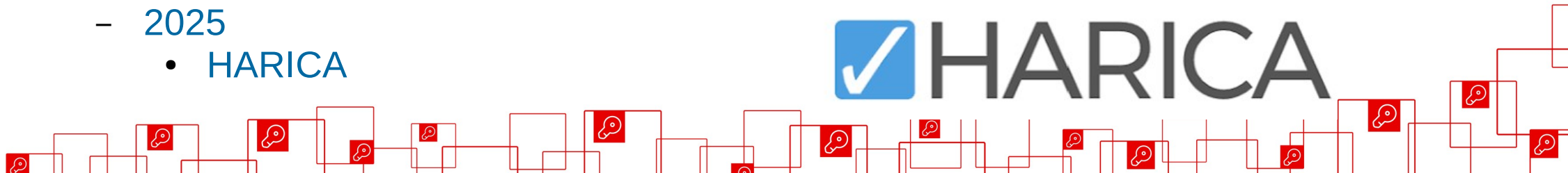


- TCS
 - Zprostředkovaná služba
 - Serverové, osobní, robotové
 - TERENA 2006 – 20. výročí
 - 2014: GÉANT
 - TERENA → Trusted Certificate Service



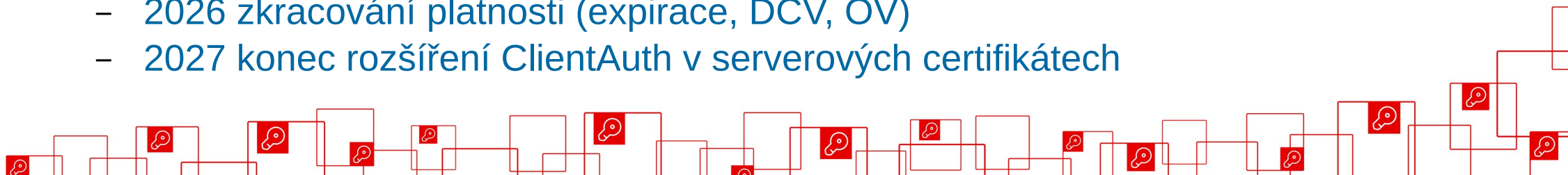


- Historie
 - 2006
 - SureServerEdu, GlobalSign
 - Serverové
 - 2010
 - Comodo
 - Serverové, později i osobní
 - 2015
 - Digicert
 - 2020
 - Sectigo
 - Předčasné ukončení smlouvy
 - 2025
 - HARICA

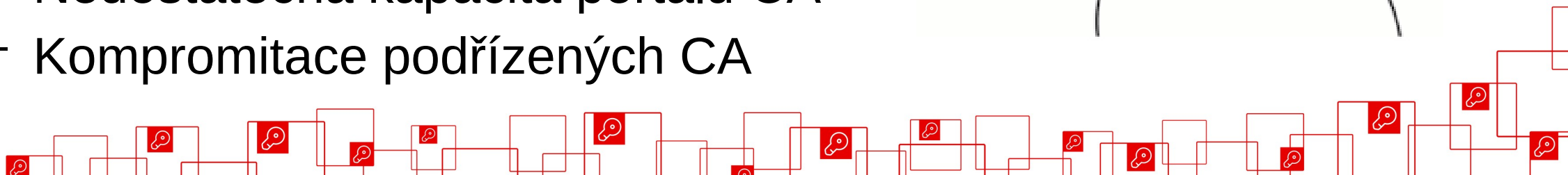




- Změny v certifikátech zavedené CA/B fórem
 - 2012 telefonické ověření organizace
 - 2013 DCV
 - 2013 konec RSA 1024b
 - 2017 konec SHA-1 (kvalifikované 2010)
 - 2017 kontrola CAA záznamů
 - 2018 OV pomocí vládního rejstříku
 - 2023 S/MIME OV
 - 2025 CAA kontrola i pro osobní certifikáty
 - 2026 konec OCSP
 - 2026 zpřísnění DNSSEC
 - 2026 zkracování platnosti (expirace, DCV, OV)
 - 2027 konec rozšíření ClientAuth v serverových certifikátech



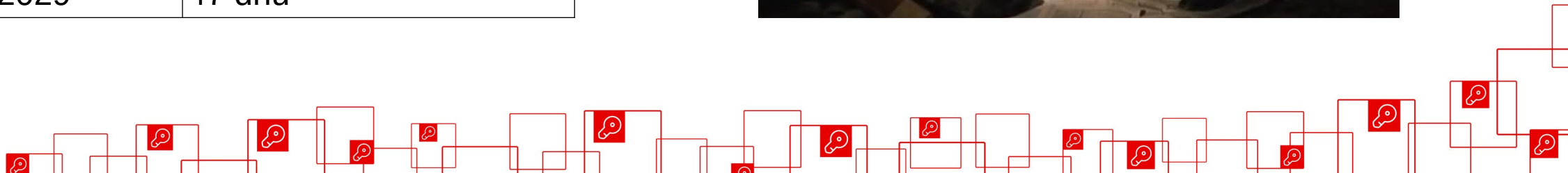
- Co se autoritám nepovedlo
 - Nezávládnuté validace
 - Blokované revokace
 - Chybně vydané certifikáty
 - Moravskosle~~z~~ký kraj
 - Rozpor s politikou
 - Nadbytečné či chybějící části předmětu
 - Nedostatečná kapacita portálu CA
 - Kompromitace podřízených CA





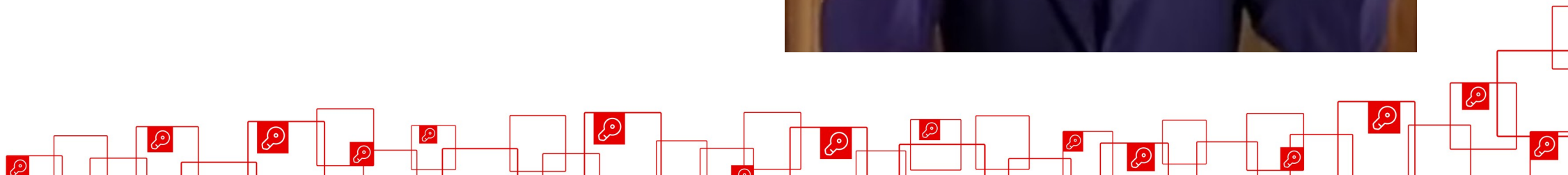
- Zkracování

Rok	Platnost
do 2012	5 – 10 let
2012	5 let
2015	3 ¼ roku
2018	2 ¼ roku
2020	398 dnů (rok a měsíc)
2026	200 dnů
2027	100 dnů
2029	47 dnů





- Jak se připravit na finální zkrácení
 - ACME, ACME, ACME!
 - Neumí? Vyhodit!
 - Wildcard? Zatím to jde.
 - SplitDNS? Proč?



**Děkuji všem za pozornost,
přeji krásný zbytek dne
a šťastnou cestu domů.**

