



Dino Paškvan

The certificate mess...

...and what to do about it

00

Introduction

01

Machine identities

01

Digital certificates are the basis of all secure connections



- HTTPS
- Mail
- VoIP
- VPN
- DNS over TLS
- Databases
- MQTT
- mTLS

02

How did we get here?

How did we get here?



1988



How did we get here?



1994-1999

How did we get here?



2005-2015



How did we get here?



2015-2016

How did we get here?



2018-2020



How did we get here?



2024-2029

03

Why are we here?

Certificate revocation



Revocation reasons

- 0 - unspecified
- 1 - **keyCompromise**
- 2 - **cACompromise**
- 3 - affiliationChanged
- 4 - superseded
- 5 - cessationOfOperation
- 6 - certificateHold
- 8 - removeFromCRL
- 9 - privilegeWithdrawn



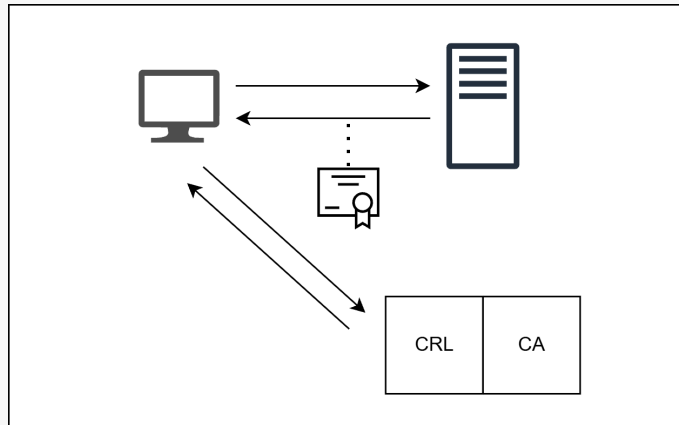


Certificate revocation

- 0 - unspecified
- 1 - **keyCompromise**
- 2 - **cACompromise**
- 3 - affiliationChanged
- 4 - superseded
- 5 - cessationOfOperation

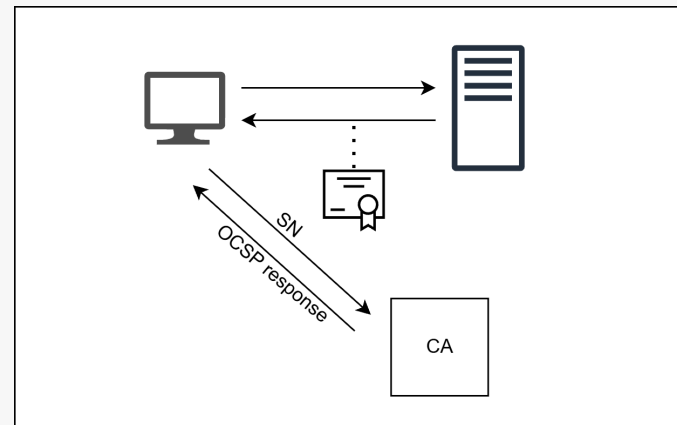
03

Why are we here?



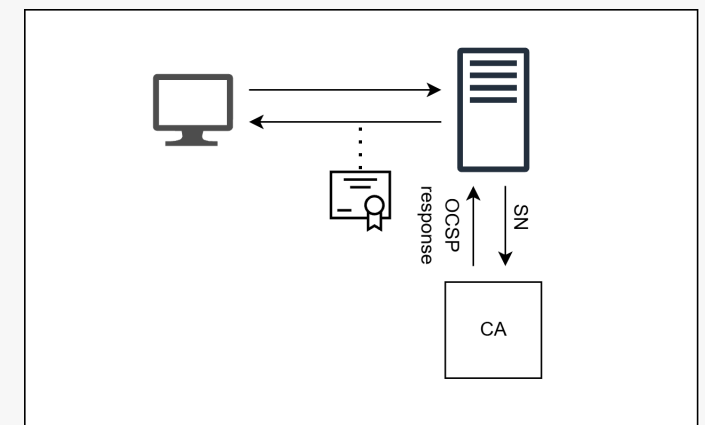
CRL

Certificate Revocation List



OCSP

Online Certificate Status Protocol

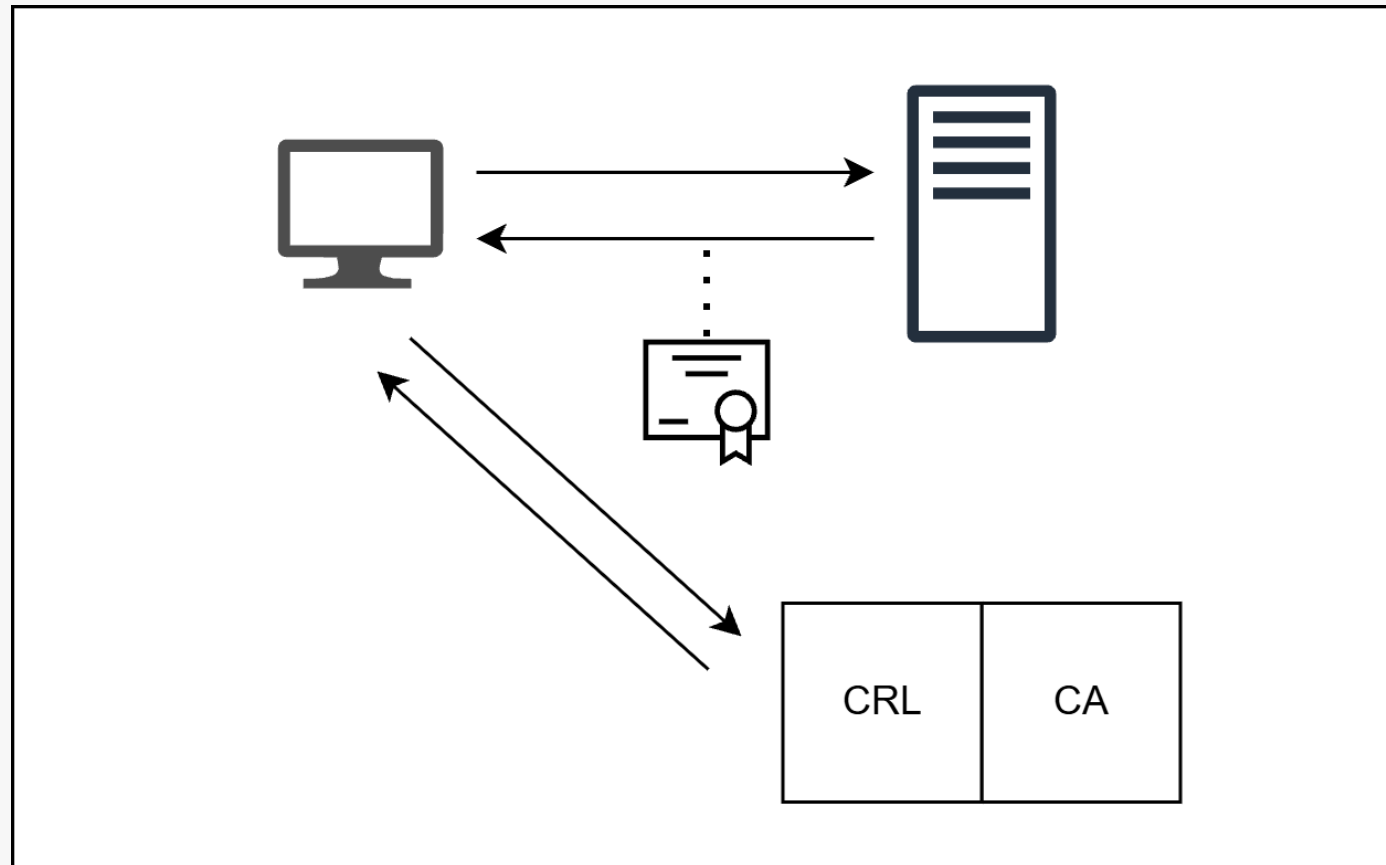


Stapled OCSP

Stapled Online Certificate Status Protocol

03

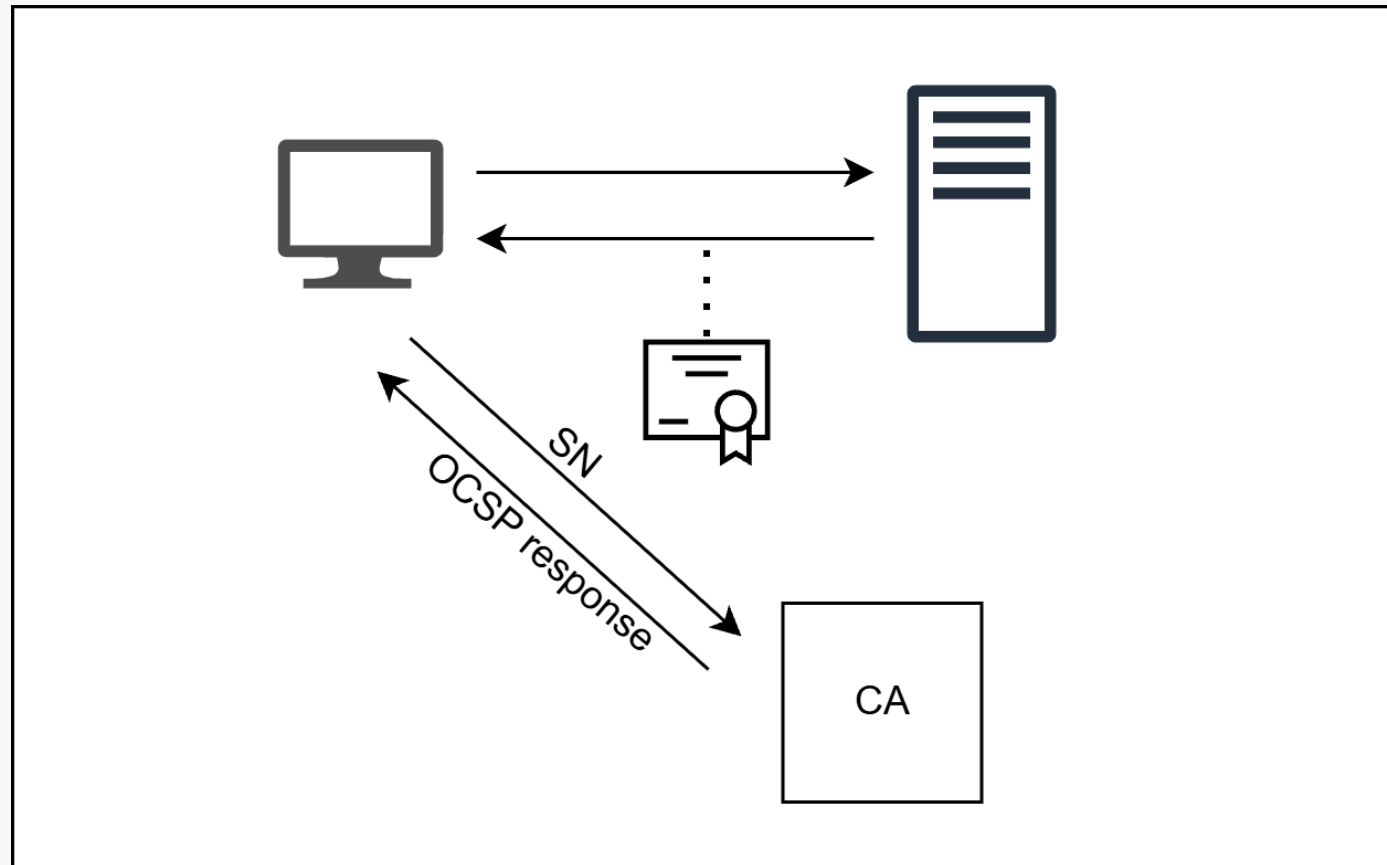
Why are we here?



CRL

03

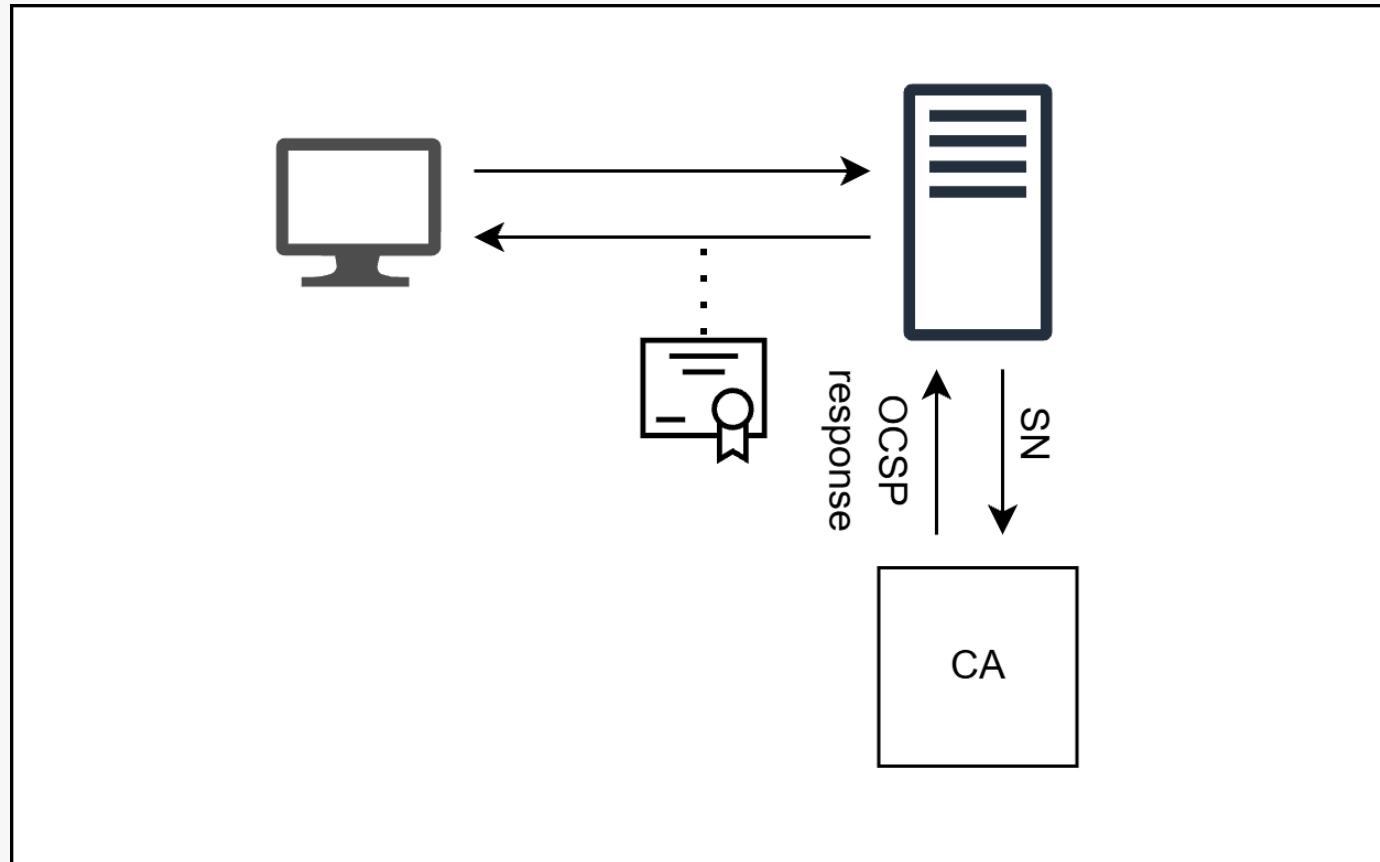
Why are we here?



OCSP

03

Why are we here?



Stapled OCSP

03

Why are we here?



47 days

04

Other challenges

04

What does a certificate actually prove?



- Domain Validation
- Organization Validation
- Extended Validation

04

What does a certificate actually prove?



- **Domain Validation**
- Organization Validation
- Extended Validation



04

What does a certificate actually prove?



- Domain Validation
- **Organization Validation**
- Extended Validation



04

What does a certificate actually prove?



- Domain Validation
- Organization Validation
- **Extended Validation**



04

What does a certificate actually prove?



- Domain Validation
- Organization Validation
- Extended Validation



04

Other factors



- PQC
- Regulatory requirements and wildcard certificates
- Let's Encrypt and 6-day certificates

05

Palo Alto Next-Generation Trust Security

05

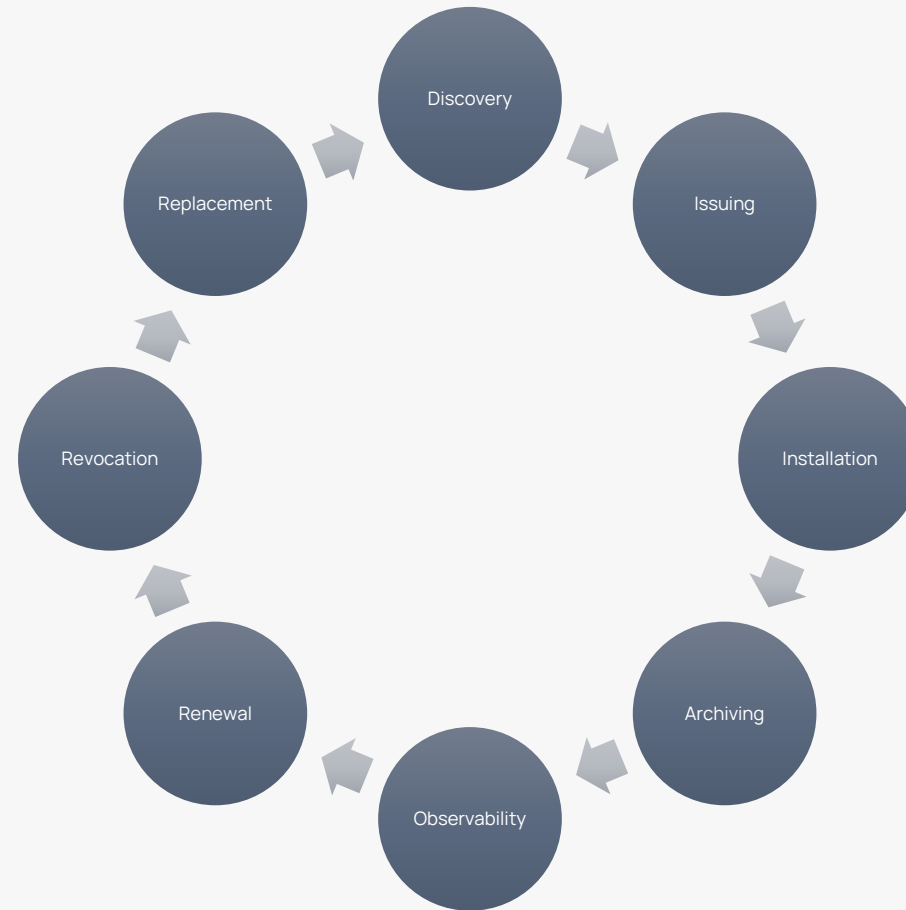
What is NGTS?



- Control plane above your CAs
- Certificate lifecycle orchestrator

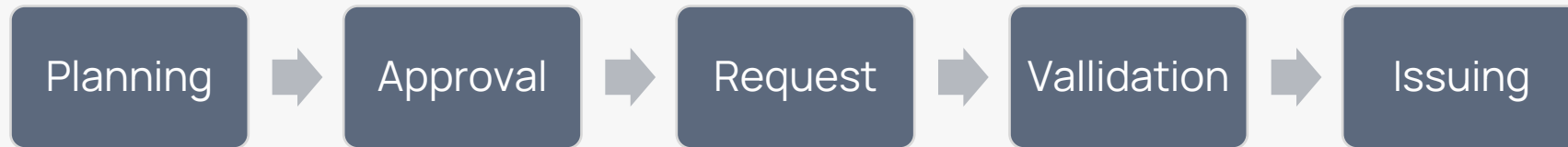


- Not a CA
- Not a replacement for existing PKI



05

Certificate lifecycle management



05

Certificate lifecycle management



Type?	Identity	Extensions
• Client • Server • Signature • ...	• CN • SAN	• Constraints • AKI • SKI

06

Automation

06

Automation



- Automating the complete lifecycle
- Requests are made according to policies
- Validation happens through CA integration
- Certificates are **not** installed manually
- Each activity is logged in an audit trail

06

CA system integrations



- Microsoft AD CS
- Sectigo
- DigiCert
- Entrust
- GlobalSign
- ACMEv2 API
- Custom integrations

06

Integrations with end devices



- Windows and Linux servers
- Orchestration platforms (Kubernetes, OpenShift...)
- Hypervisors
- Network devices
- HSM devices
- Security devices
- Custom integrations



When can we say the replacement is automated?

07

Visibility

07

Visibility



- How many certificates do you have?
- Discovery
- Discovery mechanisms
 - Network scanning
 - Passive discovery

08

Policies

08

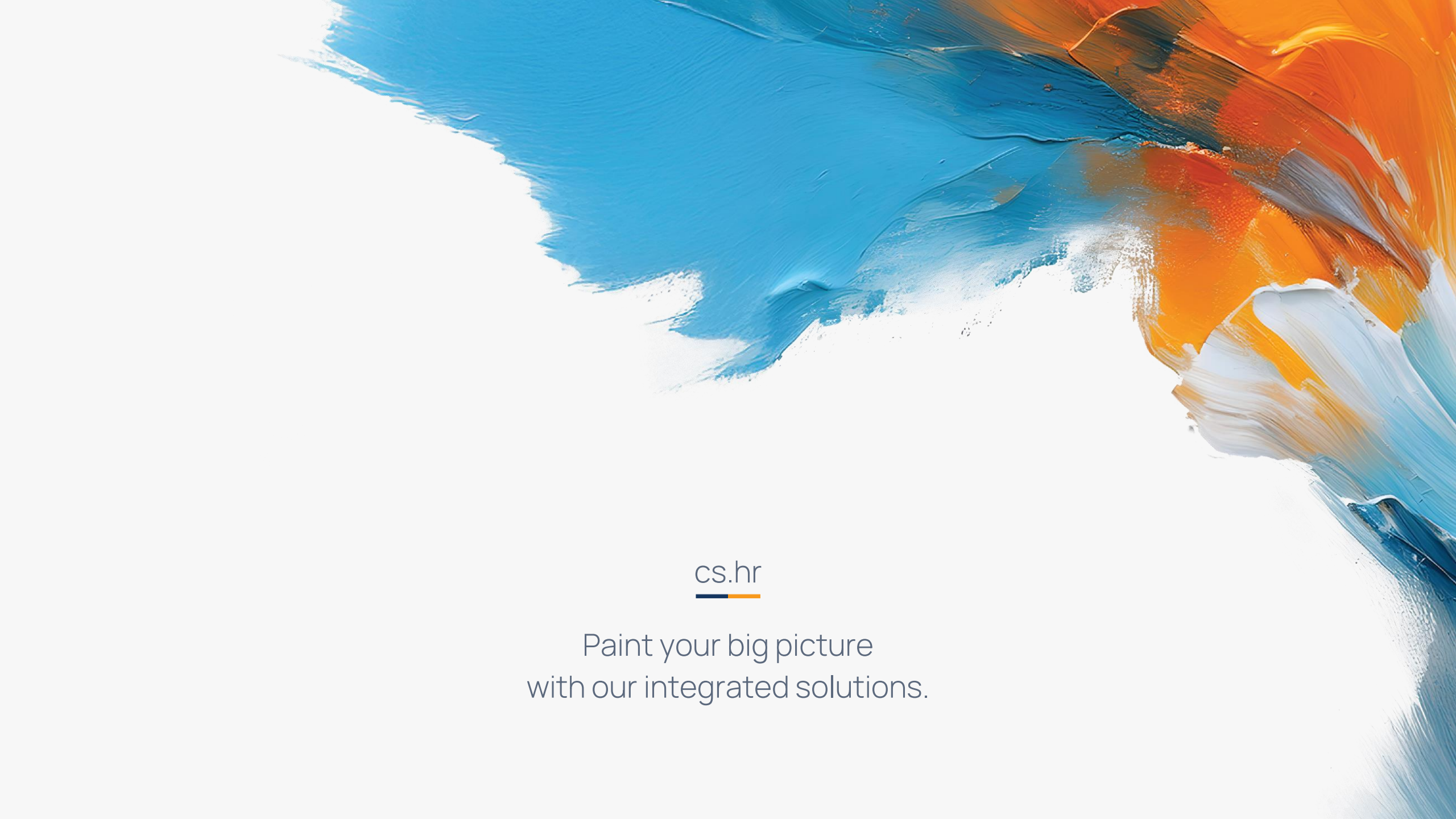
Policies



- Automation without policies is just faster chaos
- Rules enforced on every request
- Which CA serves a specific purpose?
- Key length?
- Naming conventions
- Approval

10

Recap



cs.hr

Paint your big picture
with our integrated solutions.