ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

Von Klartextpasswörtern und schwachen Schlüsseln: Eine Studie über LDAP-Server und ihre S/MIME-Zertifikate

Dr.-Ing. Fabian Ising [1, 2]
Gurur Öndarö, M. Sc.[1, 2, 3]

[1] Fraunhofer SIT
[2] ATHENE – Nationales Forschungszentrum für Angewandte Cybersicherheit
[3] FH Münster

SLAC 2026

Who are we?

Dr.-Ing. Fabian Ising

- Post-Doc at Fraunhofer SIT
- Dep. Department Head Applied Cryptography and Medical IT Security
- Group Leader: Advanced Cryptographic Engineering
- ~8 years of research experience in email security

Gurur Öndarö, M.Sc.

- PhD student at FH Münster & Fraunhofer SIT
- Topics:
  - LDAP
  - S/MIME

Who are we?
Fraunhofer SIT – Department ACM

- Fraunhofer-Institut für Sichere Informationstechnologie
  - Located in Darmstadt
  - Involved in:
    - National Research Center for Applied Cybersecurity ATHENE
    - Lernlabor Cybersicherheit
- Applied Cryptography and Medical IT Security
  - Located in Steinfurt, NRW (Campus of FH Münster)
  - Topics:
    - Applied Cryptography (Email, TLS, ...)
    - Medical IT Security

Who are you?

Wer von Euch betreibt einen LDAP-Server?

Wer von Euch betreibt eine eigene S/MIME-PKI?

Background:
How did we and up here?

November 18th, 2022

Christoph Saatjohann VIP 2:35 PM

Habe jetzt das komplette TI-KIM-ldap gedumped. 395.000 Einträge, 582.000 SMime Zertifikate.

Sebastian Schinzel VIP 4:54 PM

DU HAST WAAAS??

geil

Background:
How did we and up here?

November 18th, 2022

Christoph Saatjohann VIP 2:35 PM

Habe jetzt das komplette TI-KIM-ldap gedumped. 395.000 Einträge, 582.000 SMime Zertifikate.

Sebastian Schinzel VIP 4:54 PM

DU HAST WAAAS??

geil

37C3: Schlüssel für E-Mail-Dienst KIM für das Medizinwesen mehrfach vergeben

Background:
How did we and up here?

November 18th, 2022

Christoph Saatjohann VIP 2:35 PM

Das IAM-Betriebsteam hat mir mitgeteilt, dass am 07.06.2023 von einer IP aus unserem Netz mehrere tausend Zertifikate über die Webseite .fraunhofer.de abgerufen wurden. Die Logfiles lassen auf eine Art Crawler deuten, da die Abfrage mit fortlaufenden Nummern durchgeführt wurde (/search/cert/3016, /search/cert/3017, ...). Aufgrund der Masse wurde der Zugriff blockiert und das Betriebsteam automatisch informiert. Sie gehen aktuell von einem Angriff aus.

Die IP lässt sich auf Ihren Laptop im VPN zurückführen. Können Sie sich diesen Zugriff erklären?

Sebastian Schinzel VIP 4:54 PM

DU HAST WAAAS??

Medizinwesen mehrfach vergeben

Background:
How did we and up here?

November 18th, 2022

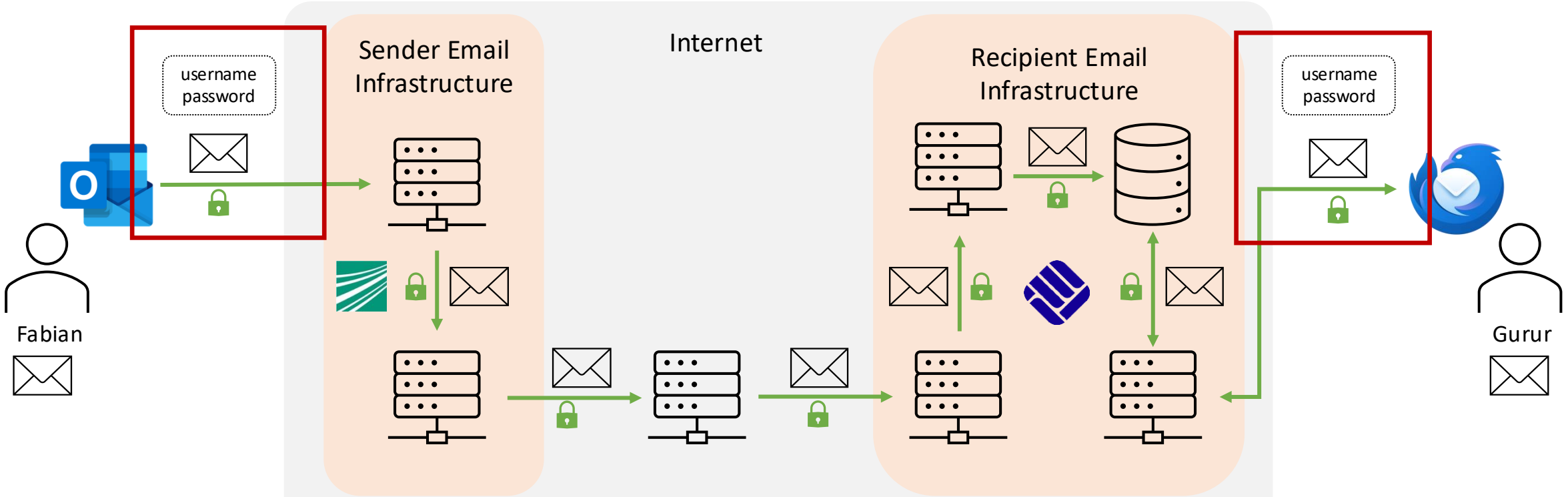
Sebastian Schinzel VIP 4:54 PM

DU HAST WAAAS??

Gurur Öndarö Dec 12th, 2023 at 9:54 PM

Das Capabilites Script hat während des Scans Samples von LDAP-Servern heruntergeladen. Die Analyse der Samples hat Klartextpasswörter offenbart, woraufhin

Email Security

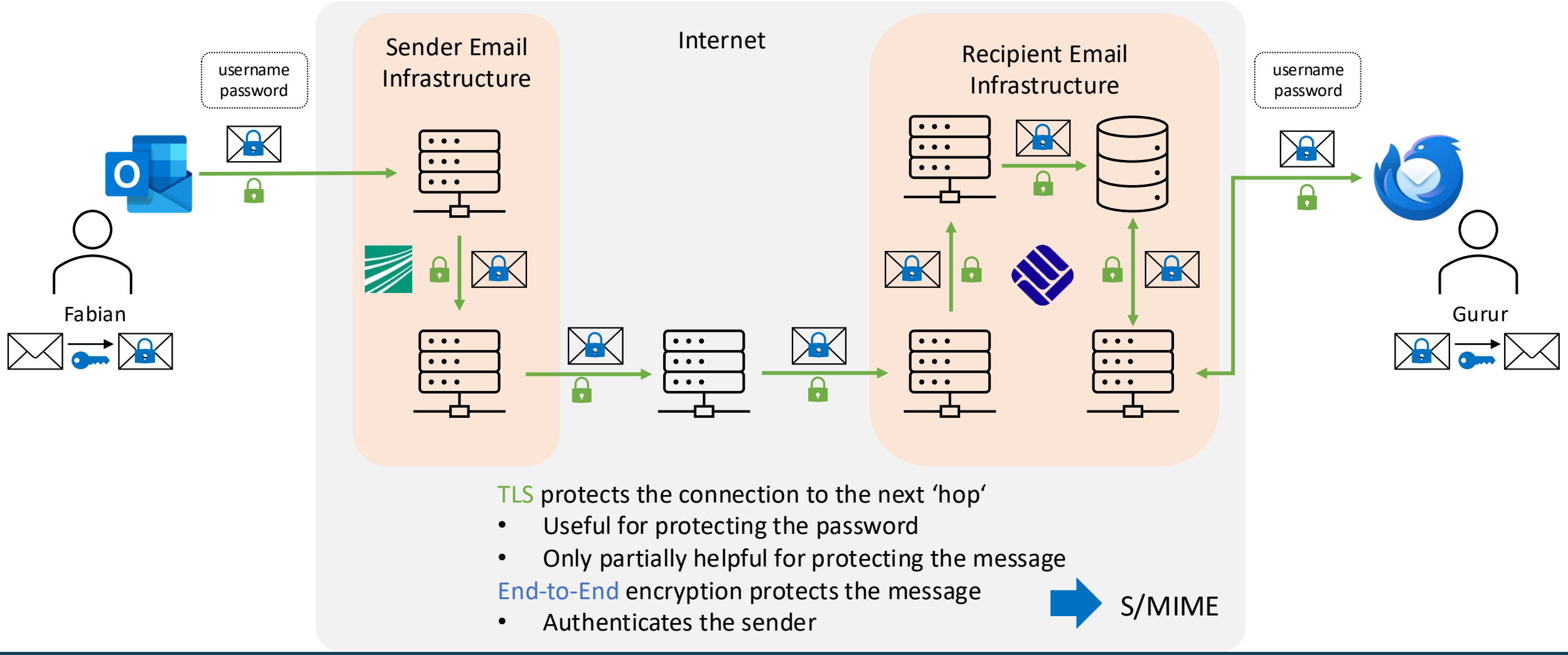


TLS protects the connection to the next ‘hop‘

- Useful for protecting the password
- Only partially helpful for protecting the message

SLAC 2024

Email Security



TLS protects the connection to the next ‘hop‘

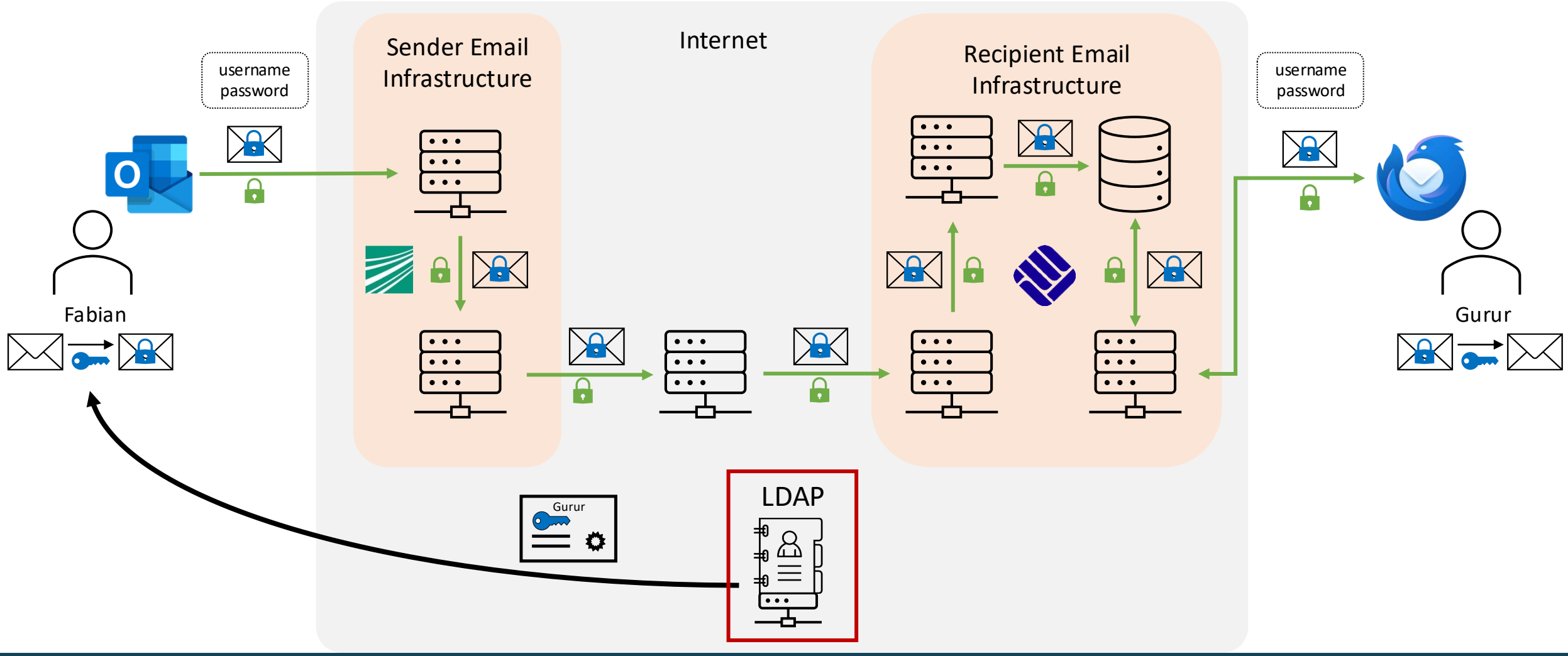
- Useful for protecting the password
- Only partially helpful for protecting the message

End-to-End encryption protects the message

- Authenticates the sender

→ S/MIME

Email Security

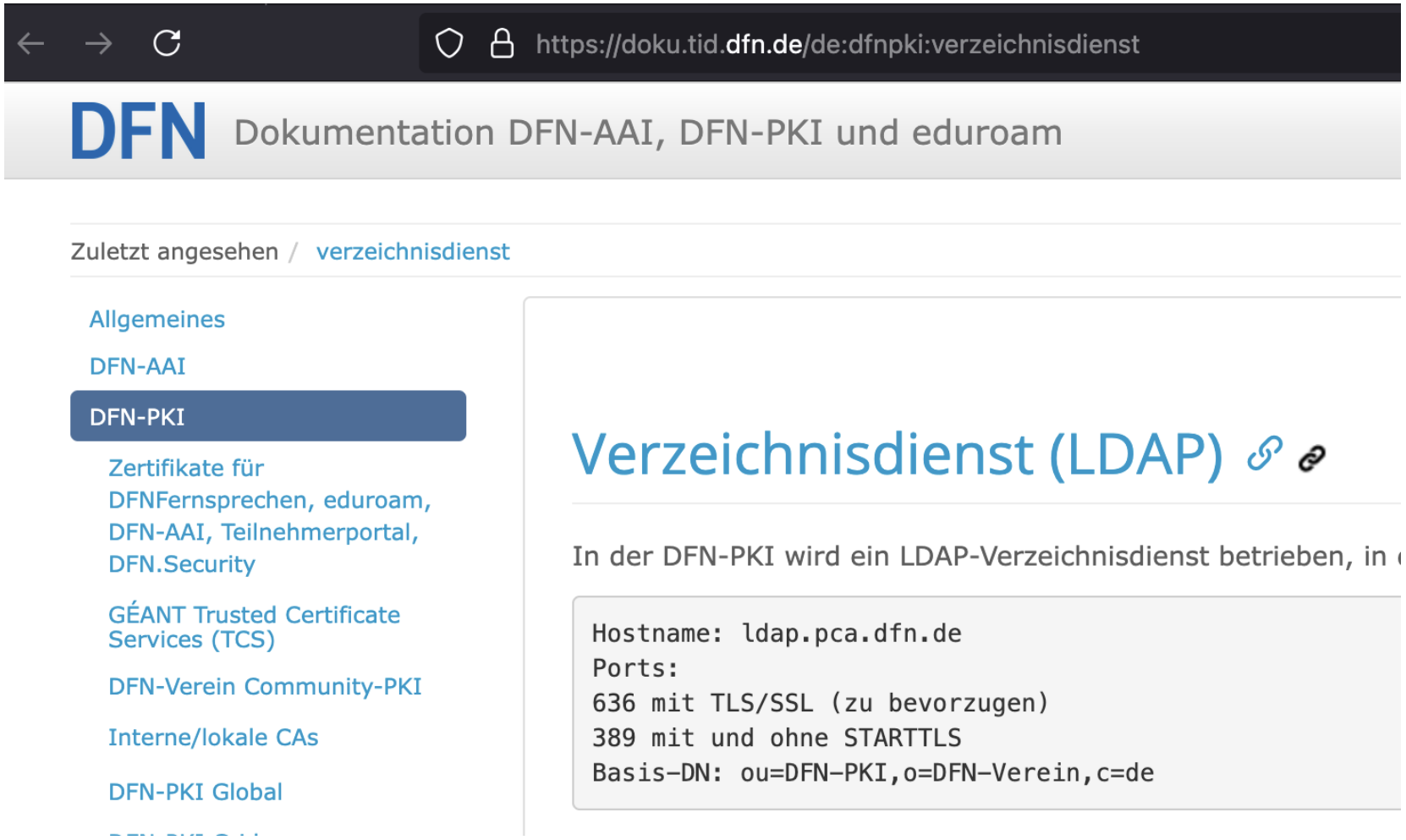


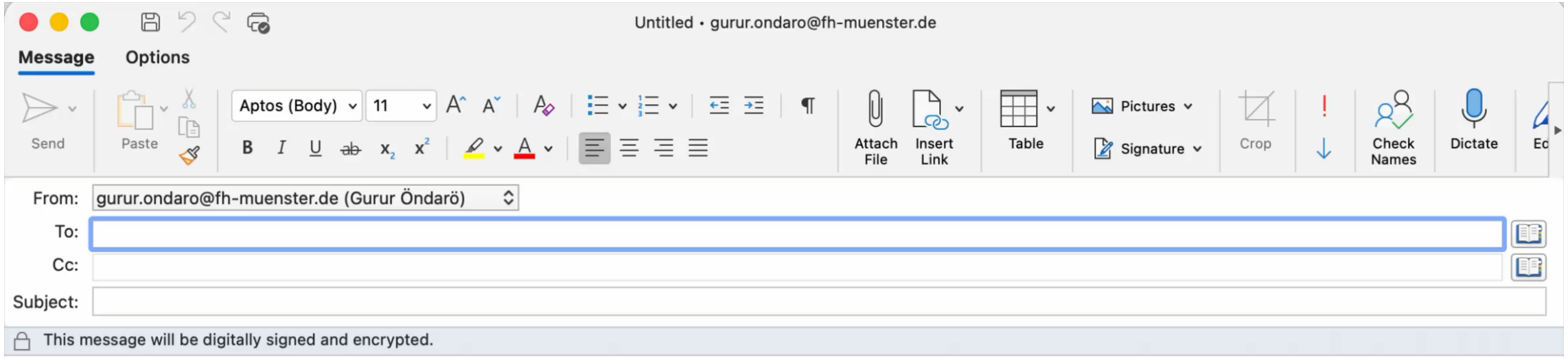
LanDscAPe:

Exploring LDAP Weaknesses and Data Leaks at Internet Scale

LDAP Background

- LDAP servers as address books
- https://doku.tid.dfn.de/de:dfnpki:verzeichnisdienst





--

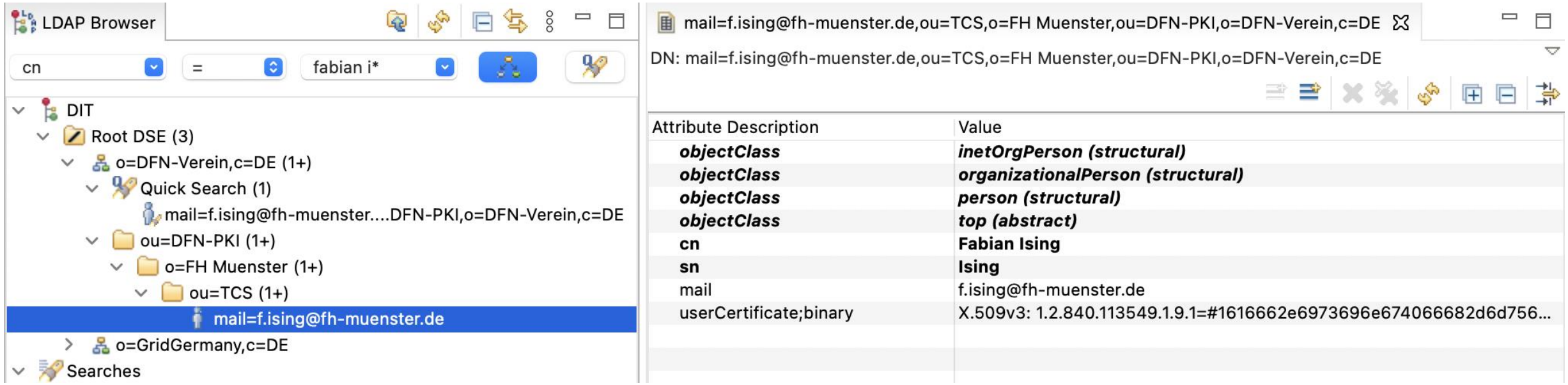
FH MÜNSTER
University of Applied Sciences

Gurur Öndarö, M. Sc.
Doktorand und wissenschaftlicher Mitarbeiter
Labor für IT-Sicherheit

FH Münster
University of Applied Sciences
Fachbereich Elektrotechnik und Informatik
Stegerwaldstraße 39, Gebäude K
48565 Steinfurt

E-Mail: gurur.ondaro@fh-muenster.de
https://www.fh-muenster.de/eti

LDAP Background



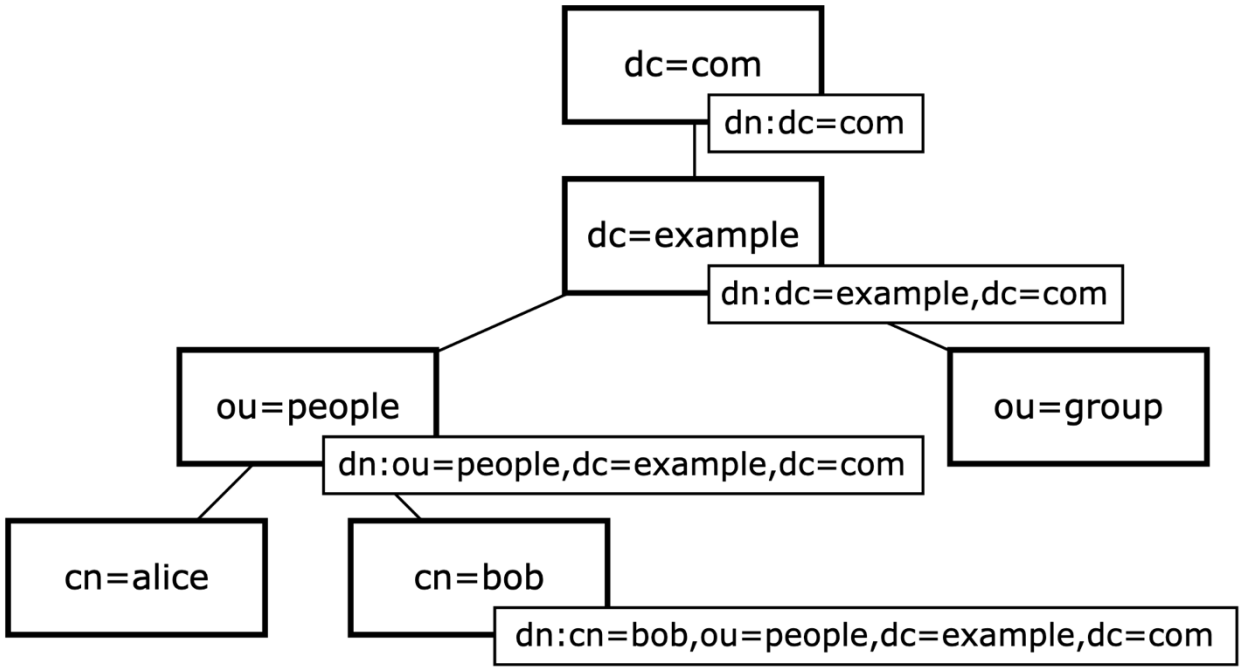
What other data is publicly accessible on LDAP servers across the Internet?

LDAP Background

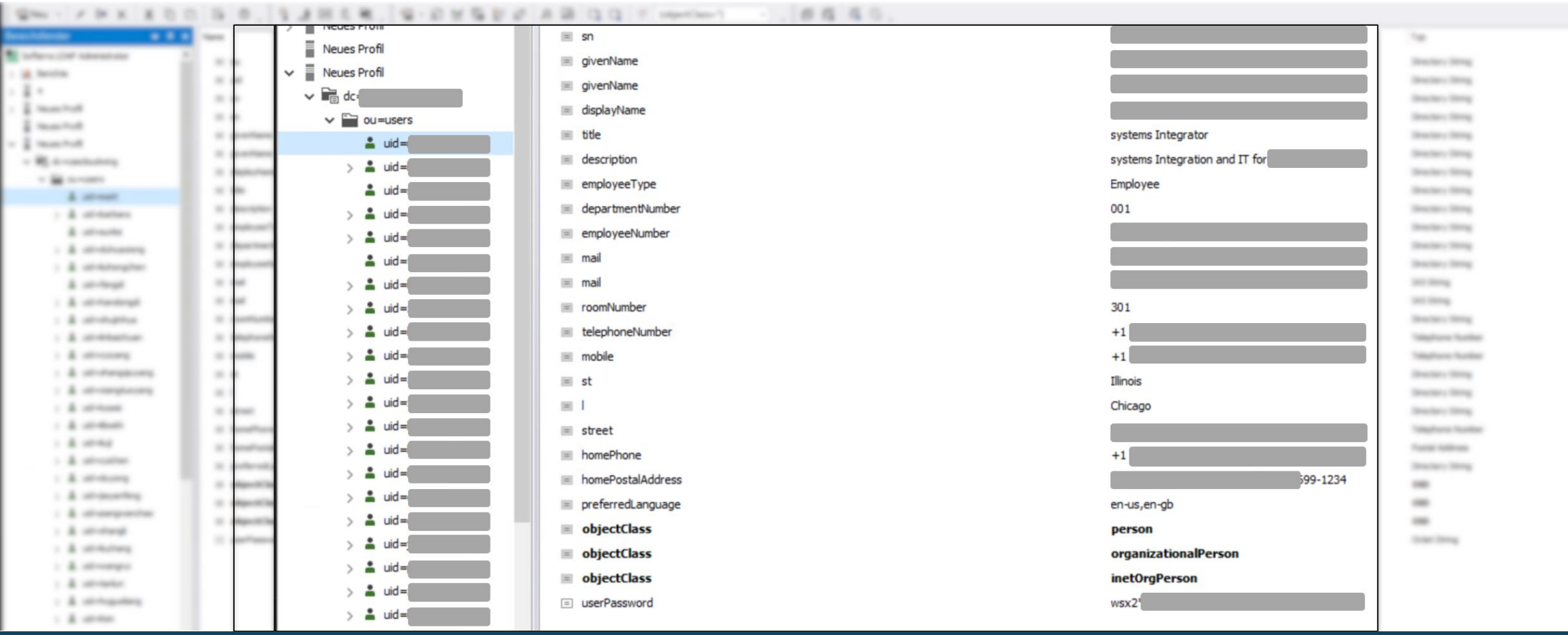
LDAP is like a weird database...

...used for

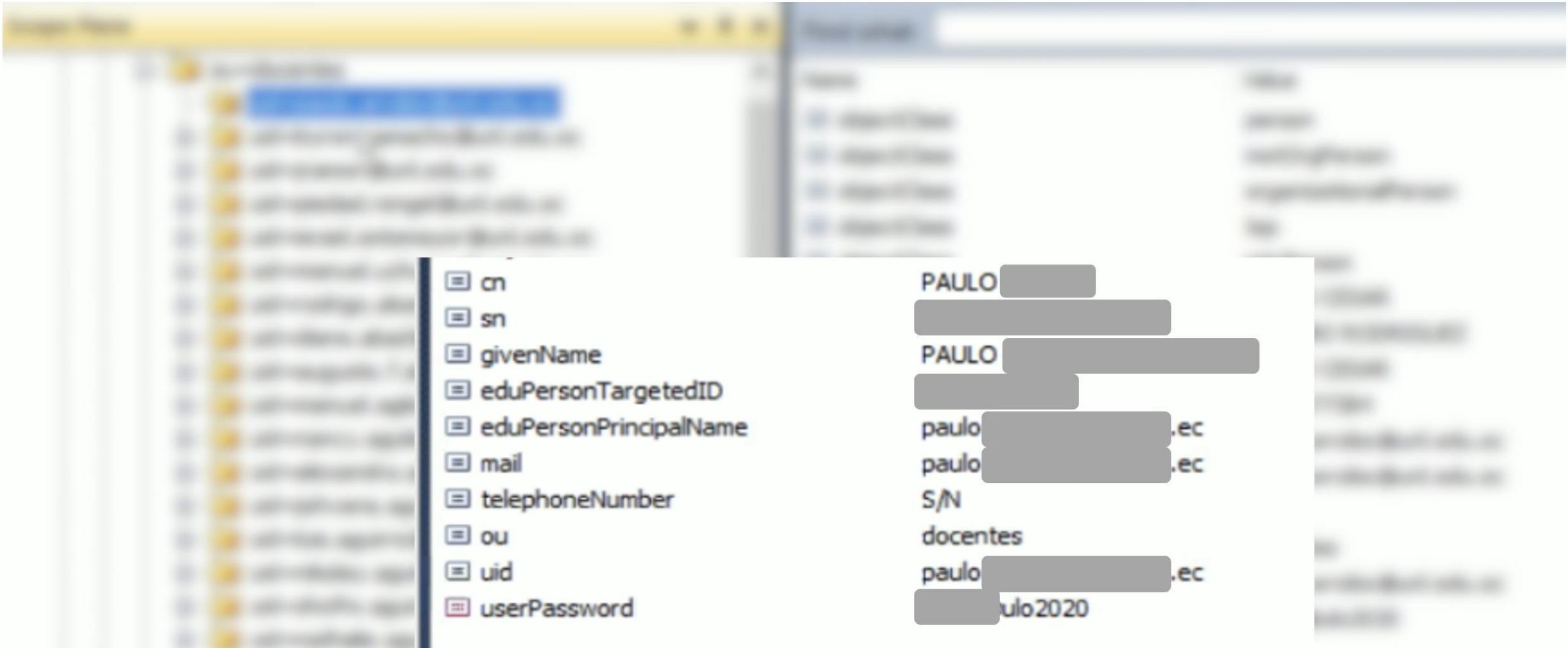
- storing personal data (address book)
- storing configuration data 😳
- their bash history 😱
- storing authentication information 🤯 !?



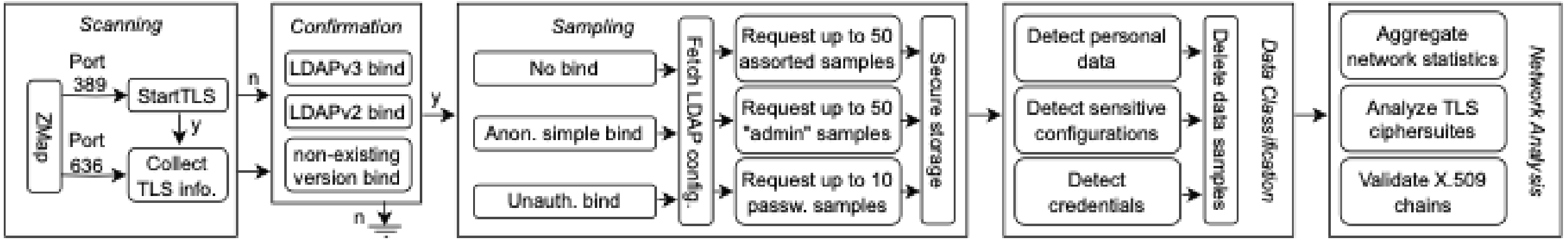
Credentials on Public LDAP Servers



Credentials on Public LDAP Servers

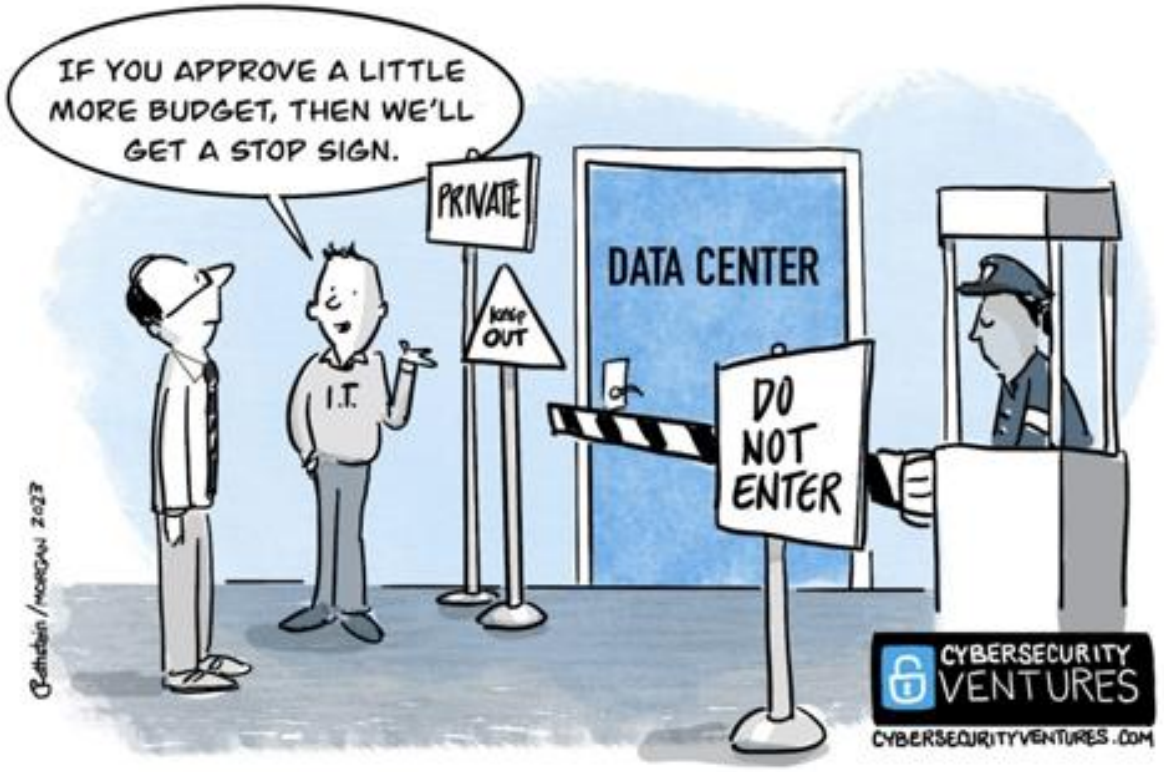


Methodology



Result: 3.7 million hosts on each port (389 and 636)
82k successful LDAP bind requests

User Data



- Limit samples
- Unique counting method
- Secured internal server with restricted access
- Data deletion
- Responsible disclosure

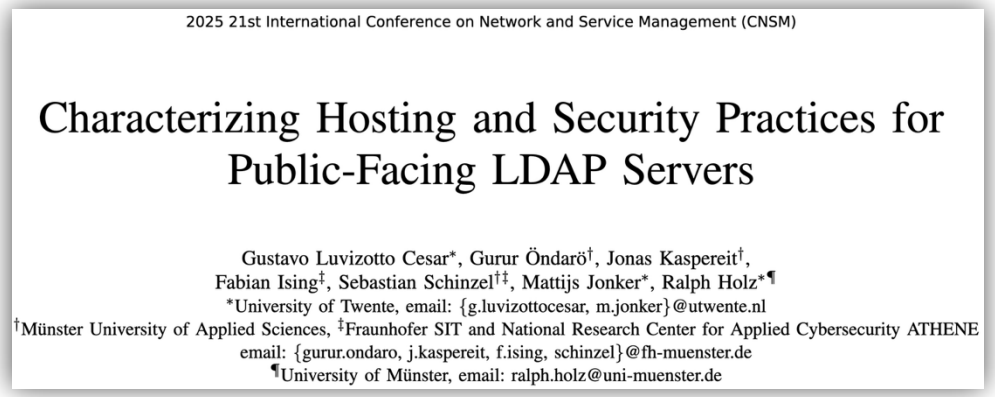
Sampling

1. Connecting to Servers 2. Fetching Configurations 3. Collecting Samples

Bind Type	Root DSE	Schema	Naming Context	Passw. Policy	Samples		
					Rand.	Admin	Passw.
Total	92,588	35,658	90,265	1,432	17,283	11,715	2,935
No bind	95.04%	87.28%	94.97%	99.93%	84.02%	99.74%	99.18%
Only Simple bind	4.93%	12.69%	5.00%	0.07%	15.98%	0.26%	0.82%
Only Unauth. bind	0.03%	0.03%	0.03%	0.00%	0.00%	0.00%	0.00%

Sampling

- Active Directory and OpenLDAP are the most widely used LDAP server implementations



2025 21st International Conference on Network and Service Management (CNSM)

Characterizing Hosting and Security Practices for Public-Facing LDAP Servers

Gustavo Luvizotto Cesar*, Gurur Öndarö†, Jonas Kaspereit†,
Fabian Ising‡, Sebastian Schinzel†‡, Mattijs Jonker*, Ralph Holz*¶
*University of Twente, email: {g.luvizottocesar, m.jonker}@utwente.nl
†Münster University of Applied Sciences, ‡Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE
email: {gurur.ondaro, j.kaspereit, f.ising, schinzel}@fh-muenster.de
¶University of Münster, email: ralph.holz@uni-muenster.de

Name	All
Category 1: Active Directory/Windows	
...MS ADC on Windows Server 2016/2019	24.6k
...MS ADC on Windows Server 2012 R2	4.9k
...MS ADC on Windows Server 2008 R2	2.7k
...MS ADC on Windows Server 2022	1.4k
...MS ADC on Windows Server 2000	0.8k
...MS ADC on Windows Server 2012	0.6k
...MS ADC on Windows Server 2008	0.3k
...Remainder in this category	0.6k
Category 2: OpenLDAP	25.0k
Category 3: Less common products	
...Kerio Connect	4.8k
...389 Directory Server	1.8k
...VMware PSC	1.3k
...Remainder in this category	0.4k
Category 4: no identification possible	5.6k
Total	74.7k

Data Classification

Personal Data	# IPs	Plaintext only	TLS config	
			w/ issues	w/o issues
Total	12,179	4,801	5,986	1,392
Last Name	89.86%	39.19%	49.01%	11.80%
Email	65.34%	36.55%	50.09%	13.36%
First Name	64.41%	37.92%	51.84%	10.24%
Full Name	49.50%	27.41%	60.24%	12.36%
Phone No.	26.83%	37.82%	47.92%	14.26%
Public Key	14.90%	23.25%	62.04%	14.71%
Location	10.54%	50.55%	32.01%	17.45%
Job	10.17%	33.28%	45.96%	20.76%
Address	10.14%	44.21%	33.36%	22.43%
Title	9.93%	39.04%	35.65%	25.31%
Country	7.45%	58.77%	29.33%	11.91%
Photo	2.82%	47.23%	35.28%	17.49%
Birthday	1.45%	21.02%	47.73%	31.25%
Gender	0.62%	54.67%	38.67%	6.67%
SSN	0.16%	21.05%	78.95%	0.00%

Personal data attributes exposed by LDAP servers.
Percentages based on the corresponding number of IPs.

Data Classification

- 26,464 servers support SASL
- 9,731 servers leak internal information
- 616 servers are vulnerable to existing CVEs

Fast Track to Admin

- 1,817 LDAP servers exposed credentials
- > 32% leaked plausible plaintext passwords
- > 3.9 million credentials publicly accessible
- 526 servers leaked passwords where the username contained the substring 'admin'

Network Analysis

	Total IPs	Leak credentials	Personal data	SASL support	CVE	Internal info.
Supporting TLS	48,198 (100%)	910 (100%)	7,378 (100%)	18,502 (100%)	528 (100%)	7,118 (100%)
TLSv1.3	36.67%	20.00%	27.24%	42.04%	28.41%	49.34%
TLSv1.2	59.46%	77.03%	68.91%	55.92%	71.59%	46.90%
TLSv1.1	0.33%	0.33%	0.16%	0.23%	0.00%	0.10%
TLSv1.0	3.54%	2.64%	3.69%	1.81%	0.00%	3.67%
Recommended cipher suites	65.92%	36.59%	44.20%	57.49%	94.89%	61.42%
Other cipher suites	34.08%	63.41%	55.80%	42.51%	5.11%	38.58%
. . . with RSA key exchange	24.27%	57.14%	53.71%	41.77%	5.11%	36.93%
. . . using CBC	12.26%	8.35%	6.30%	3.64%	5.11%	5.49%
. . . using 3DES	0.31%	0.00%	0.03%	0.00%	0.00%	0.00%
Valid Cert. Chain	36.81%	17.69%	24.10%	40.38%	32.20%	47.78%
Invalid Cert. Chain	63.19%	82.31%	75.90%	59.62%	67.80%	52.22%
... Self-signed	32.30%	21.87%	22.61%	16.53%	1.70%	10.97%
... Expired/not yet valid	19.65%	43.63%	35.52%	25.15%	6.63%	14.34%
... Unknown authority	11.20%	16.70%	17.74%	17.91%	59.28%	26.89%

Disclosure

- Disclosure Campaign February 2024
- 475 (26.1%) of credential-leaking servers were no longer available
- **5 servers** have been switched to authenticated access

LDAP Takeaways

- Findings
  - 15% of public LDAP servers are leaking personal data
  - 12% of public LDAP servers are leaking internal information
  - Around 3.9 million user credentials, including cleartext passwords, are exposed
  - Most LDAP servers have no proper TLS configuration

LDAP Takeaways

- Improperly encrypted LDAP traffic may leak data and communication patterns
- LDAP directories are a valuable source for phishing attacks
- Misconfigured LDAP servers may expose user and even admin credentials

- Use TLS to prevent traffic interception & manipulation
- Regularly check LDAP servers for unintended Internet exposure
- Regularly review configurations for anonymous access and exposed attributes

Reference

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

LanDscAPe: Exploring LDAP Weaknesses and Data Leaks at Internet Scale

Jonas Kaspereit and Gurur Öndarö, *Münster University of Applied Sciences;* Gustavo Luvizotto Cesar, *University of Twente;* Simon Ebbers, *Münster University of Applied Sciences;* Fabian Ising, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Christoph Saatjohann, *Münster University of Applied Sciences, Fraunhofer SIT, and National Research Center for Applied Cybersecurity ATHENE;* Mattijs Jonker, *University of Twente;* Ralph Holz, *University of Twente and University of Münster;* Sebastian Schinzel, *Münster University of Applied Sciences, Fraunhofer SIT, and National Research Center for Applied Cybersecurity ATHENE*

https://www.usenix.org/conference/usenixsecurity24/presentation/kaspereit

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

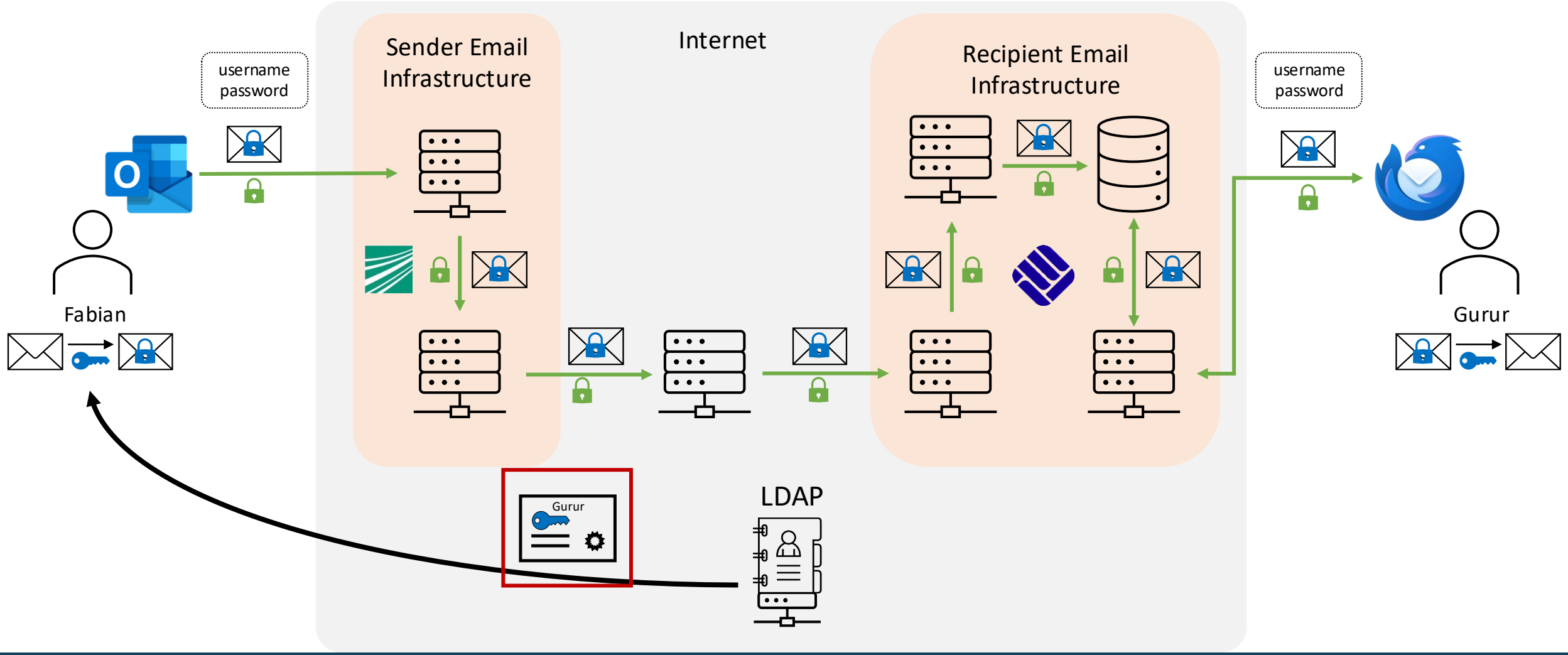
SCAN ME

Jonas Kaspereit[1], Gurur Öndarö[1,2], Gustavo Luvizotto Cesar[3], Simon Ebbers[1], Fabian Ising[2], Christoph Saatjohann[1], Mattijs Jonker[3], Ralph Holz[3,4], and Sebastian Schinzel[1,2]

[1]Münster University of Applied Sciences
[2]Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE
[3]University of Twente
[4]University of Münster

S/MINE:
Collecting and Analyzing S/MIME Certificates at Scale

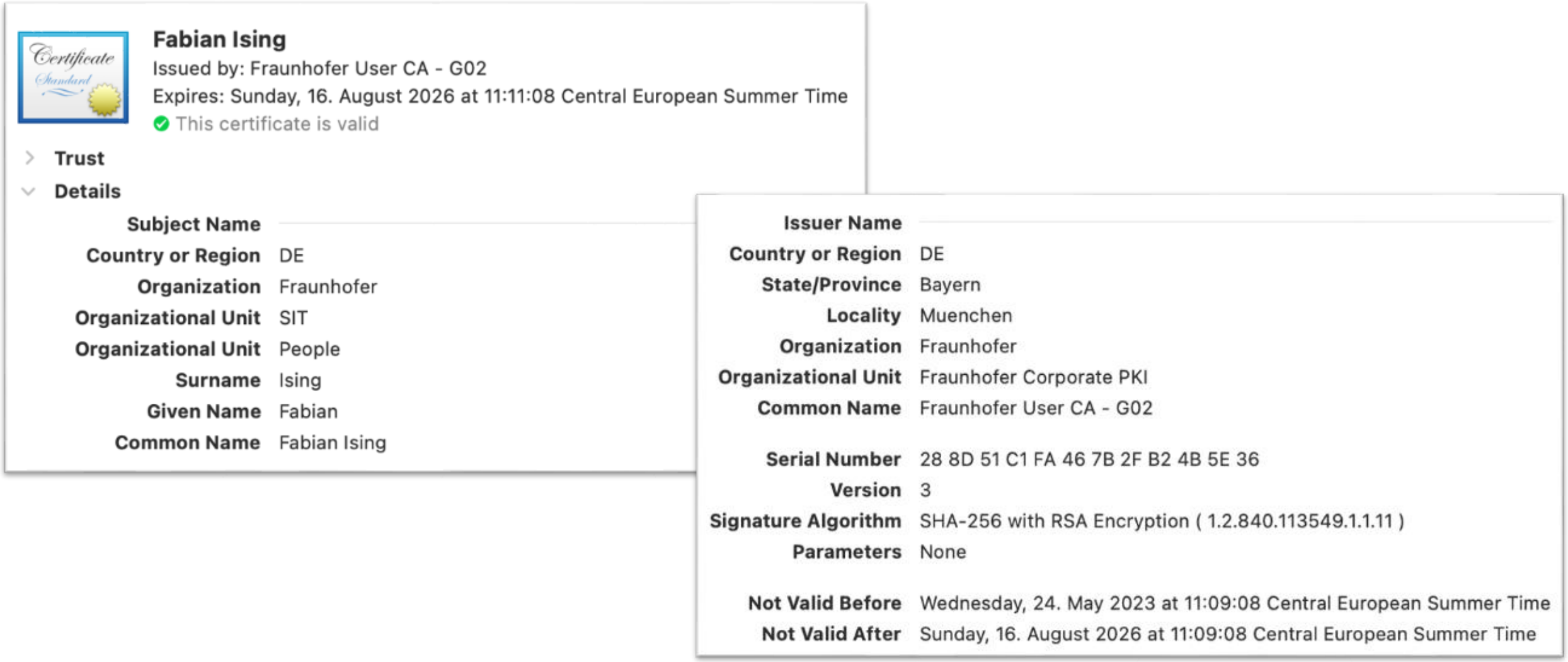
S/MIME Certificates



S/MIME – Background
X.509 Certificates

Attribute Description	Value
cn	**Fabian Ising**
displayName	Ising, Fabian
fullName	Fabian Ising
givenName	Fabian
l	Steinfurt
mail	fabian.ising@sit.fraunhofer.de
objectClass	***inetOrgPerson (structural)***
objectClass	***ndsLoginProperties (abstract)***
objectClass	***organizationalPerson (structural)***
objectClass	***Person (structural)***
objectClass	***Top (structural)***
personalTitle	Dr.
postalCode	48565
sn	**Ising**
street	Stegerwaldstraße 39
userCertificate;binary	X.509v3: CN=Fabian Ising,2.5.4.42=#0c0646616269616e,2.5.4.4=#0c054973696e67,OU=People,OU=SIT,O=Fraunhofer,C=DE

S/MIME – Background
X.509 Certificates



S/MIME – Background
X.509 Certificates

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : D5 57 6E C7 07 31 6F 86 ...
Exponent	65537
Key Size	2.048 bits
Key Usage	Verify, Wrap, Derive

Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Non-Repudiation

Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Email Protection (1.3.6.1.5.5.7.3.4)

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
RFC 822 Name	fabian.ising@sit.fraunhofer.de

S/MIME – Quiz
What is an S/MIME Certificate?

Attribute	Value
Subject Email Address	fabian.ising@sit.fraunhofer.de
Key Usage	Digital Signature, Non-Repudiation
Extended Key Usage	Email Protection
Subject Alternative Name	fabian.ising@sit.fraunhofer.de

Attribute	Value
Subject Email Address	fabian.ising@sit.fraunhofer.de
Key Usage	Key Encipherment
Extended Key Usage	Email Protection
Subject Alternative Name	fabian.ising@sit.fraunhofer.de

S/MIME – Quiz
What is an S/MIME Certificate?

Attribute	Value
Subject Email Address	-
Key Usage	Digital Signature, Non-Repudiation
Extended Key Usage	Email Protection
Subject Alternative Name	-

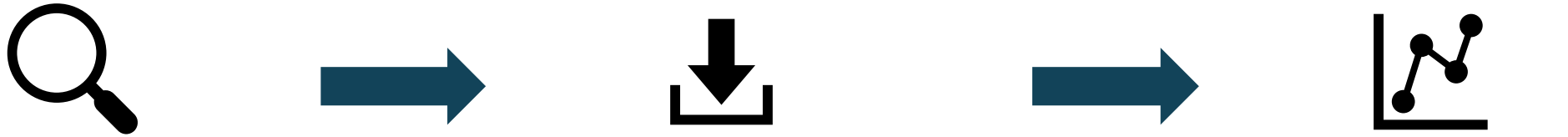
```
End-entity certificates MAY contain an Internet mail address.
```

S/MIME – Quiz
What is an S/MIME Certificate?

Attribute	Value
Subject Email Address	fabian.ising@sit.fraunhofer.de
Key Usage	Digital Signature, Non-Repudiation
Extended Key Usage	CodeSigning
Subject Alternative Name	fabian.ising@sit.fraunhofer.de

Attribute	Value
Subject Email Address	fabian.ising@sit.fraunhofer.de
Key Usage	Digital Signature, Non-Repudiation
Extended Key Usage	-
Subject Alternative Name	fabian.ising@sit.fraunhofer.de

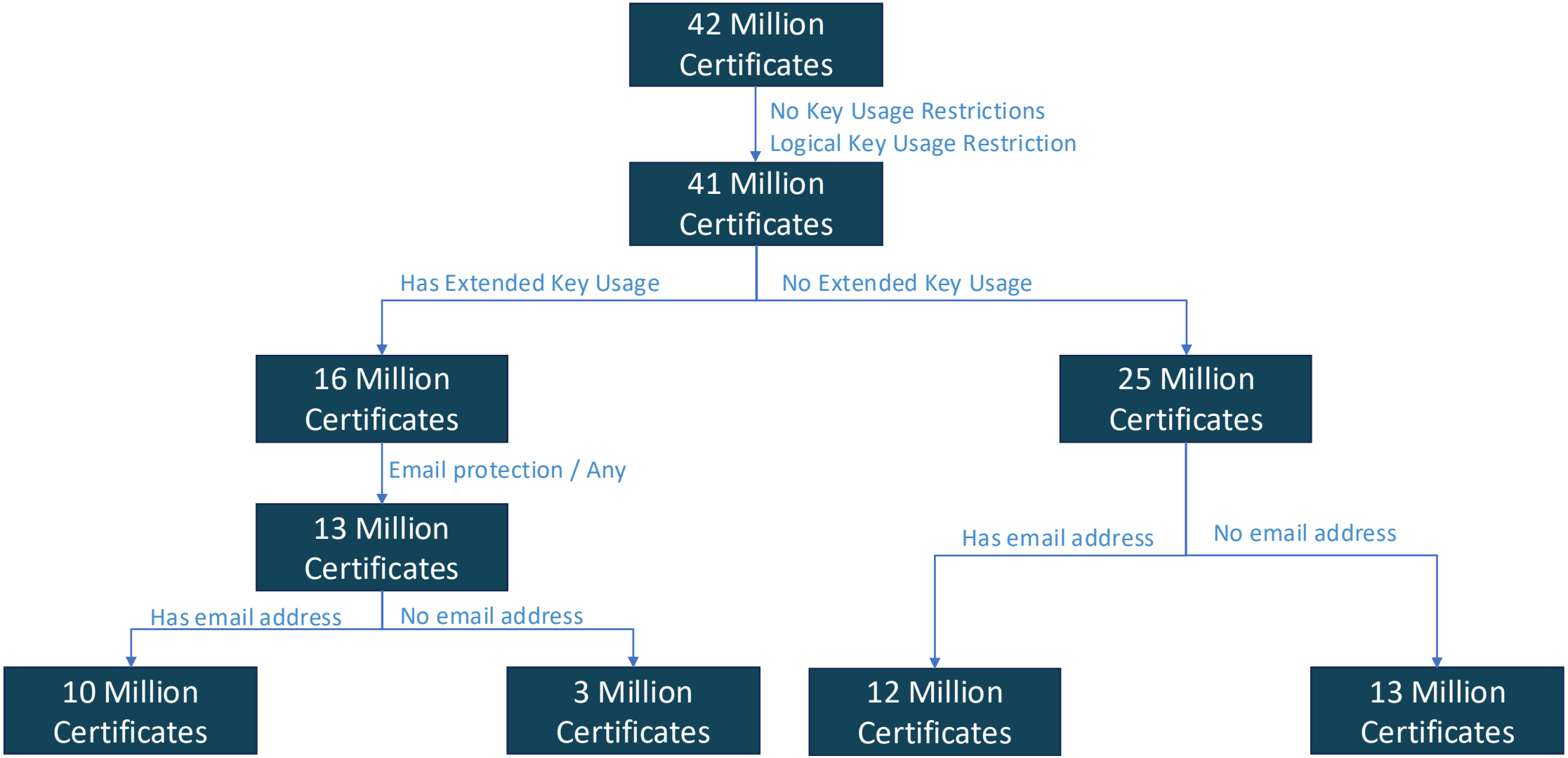
Methodology



Scan for LDAP servers → Crawl LDAP Entries → Analyze Certificates

Result: 42 Million X.509 certificates

What is an S/MIME Certificate?



What is an S/MIME certificate?

Certificate Configuration			Certificates (% of all collected)	Accepted by Email Clients				
Email Address	**Key Usage (KU)**	**Extended KU**		**Outlook macOS**	**Outlook Windows**	**Apple Mail iOS**	**Apple Mail macOS**	**Mozilla Thunderbird**
General Purpose Certificates (w/ email)			10,441,523					
yes	(DS or NR) and KE	EP	6,125,365 (14.69%)	✓	✓	✓	✓	✓
yes	(DS or NR) and KE	Any (no EP)	4 (0.0%)	$(\checkmark_e)^1$	✓	$\checkmark^4$	✗	✗
yes	(DS or NR) and KE	None	4,029,101 (9.66%)	✓	✓	✓	✓	✓
yes	None	EP	808 (0.0%)	✓	✓	✓	✗	✓
yes	None	Any (no EP)	0 (0.0%)	$\checkmark_e$	✓	$(\checkmark_s)^4$	✗	✗
yes	None	None	286,245 (0.69%)	✓	✓	✓	✗	✓
Encryption Certificates (w/ email)			3,999,548					
yes	KE	EP	1,273,769 (3.06%)	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$
yes	KE	Any (no EP)	17 (0.0%)	$(\checkmark_e)^1$	$\checkmark_e^3$	✗	✗	✗
yes	KE	None	2,725,762 (6.54%)	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$	$\checkmark_e$
Signing Certificates (w/ email)			7,944,636					
yes	(DS or NR)	EP	2,760,731 (6.62%)	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$
yes	(DS or NR)	Any (no EP)	103 (0.0%)	✗	$\checkmark_s$	$(\checkmark_s)^4$	✗	✗
yes	(DS or NR)	None	5,183,802 (12.43%)	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$	$\checkmark_s$
General Purpose Certificates w/o Email			3,796,585					
no	(DS or NR) and KE	EP	2,841,857 (6.82%)	✗	$\checkmark_s$	$\checkmark_e$	$(\checkmark_e)^2$	✗
no	(DS or NR) and KE	Any (No EP)	253 (0.0%)	✗	$\checkmark_s$	$\checkmark_e$	✗	✗
no	(DS or NR) and KE	None	954,475 (2.29%)	✗	$\checkmark_s$	$\checkmark_e$	$(\checkmark_e)^2$	✗

S/MIME Baseline Requirements Overview

- List of technical and non-technical requirements for operating a publicly trusted S/MIME CA
- Caveat: Apply only to **public** CAs
- Split into three profiles:
  - Strict: Only for S/MIME
  - Multipurpose: Certificates for S/MIME and other purposes (e.g., Document Signing)
  - Legacy: Fallback

Certificate Consumers

- Apple
- Google
- Microsoft
- Mozilla
- Mozilla/Thunderbird
- Posteo e.K.
- rundQuadrat
- Zertificon

Certification Authorities

- AC Camerfirma SA
- AC Firmaprofessional SA
- Actalis S.p.A.
- Asseco Data Systems SA (Certum)
- CFCA
- Chunghwa Telecom
- Comsign
- DigiCert
- Disig
- D-TRUST
- eMudhra
- Entrust
- GDCA
- GlobalSign
- GlobalTrust
- HARICA
- IdenTrust
- iTrusChina
- MSC Trustgate Sdn Bhd
- OISTE Foundation
- SECOM Trust Systems
- Sectigo
- SHECA
- SSC
- SSL.com
- SwissSign
- Telia Company
- TrustAsia
- TWCA
- Visa

S/MIME Baseline Requirements

This S/MIME Baseline Requirements document describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary for the issuance and management of Publicly-Trusted S/MIME Certificates.

An S/MIME Certificate for the purposes of this document can be identified by the existence of an Extended Key Usage (EKU) for `id-kp-emailProtection` (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of a `rfc822Name` or an `otherName` of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension.

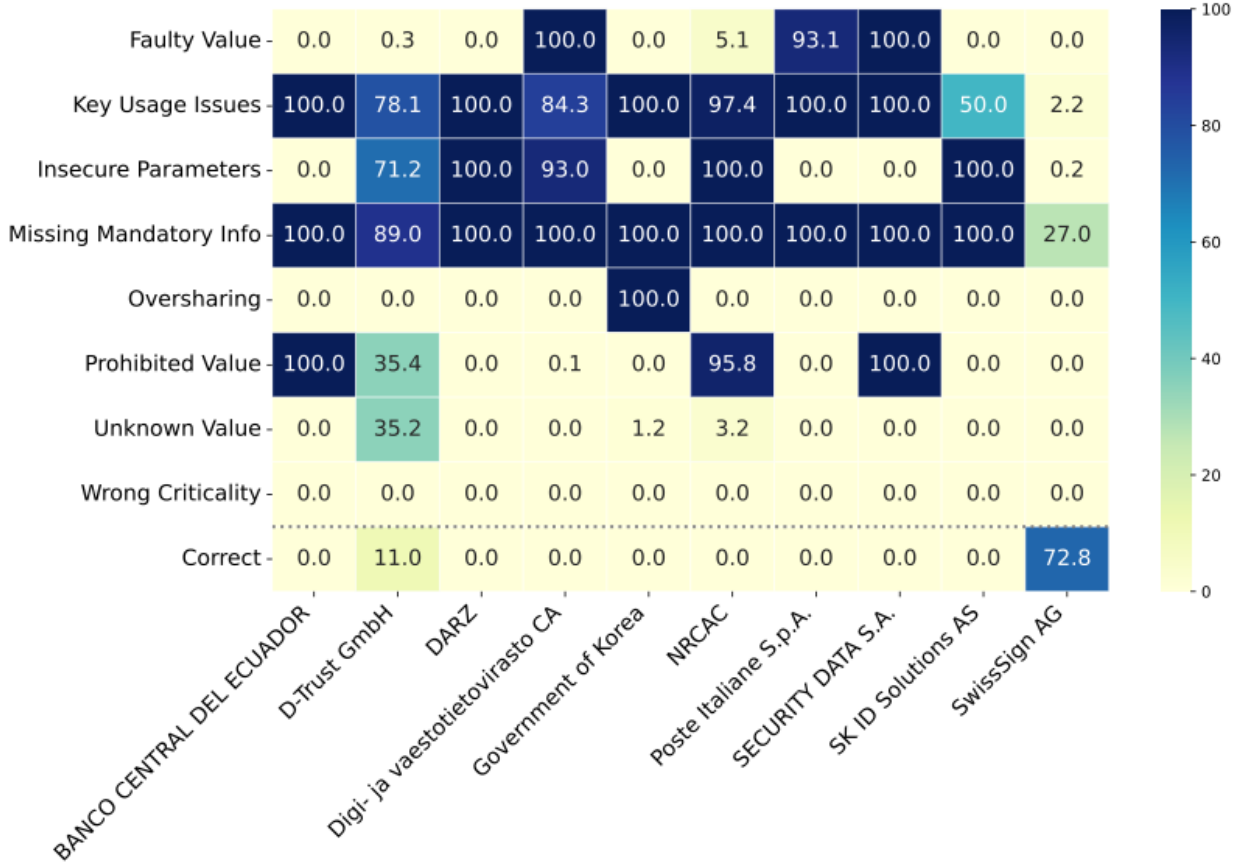
S/MIME Baseline Requirements
Technical Requirements (Excerpt)

- Extended Key Usage:
  - Strict: emailProtection
  - Multipurpose/Legacy: emailProtection + X
- Validity periods:
  - Multipurpose/Strict: 825 days (~2 years + 3 months)
  - Legacy: 1.185 days (~3 years + 3 months)
- Stronger Algorithms:
  - No SHA-1
  - No RSA-1024
- Robust Revocation Infrastructure

Baseline Requirements

- Adoption of S/MIME BR is slow but steady:
  - ~ **20 distinct CAs** issued compliant certificates (01/23 - 04/25)

- Most common problems:
  - Missing information:
    - Email address
    - Revocation info
  - No Extended Key Usage
  - Overly long validity



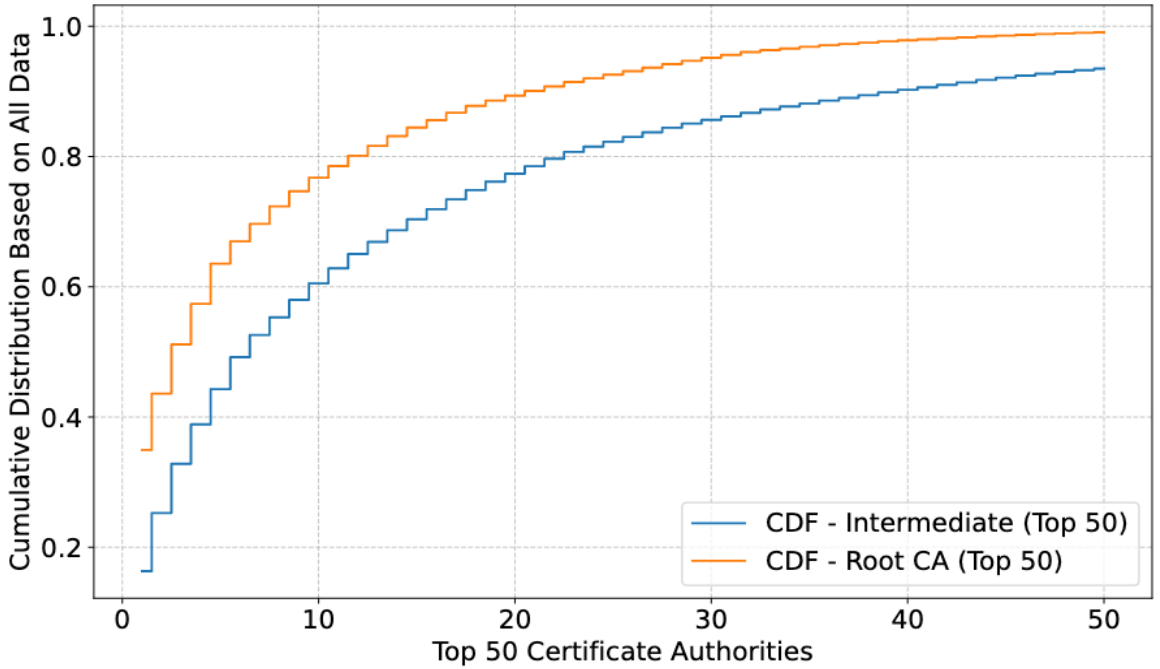
Top 10 Root CAs. Percentage of Errors by Root CA for Certificates issued since 01/2023

Certificate Trust

- How do you know if a certificate is trustworthy?

- Great! But where do I get the Issuer certificate?

Who issues all those certificates?



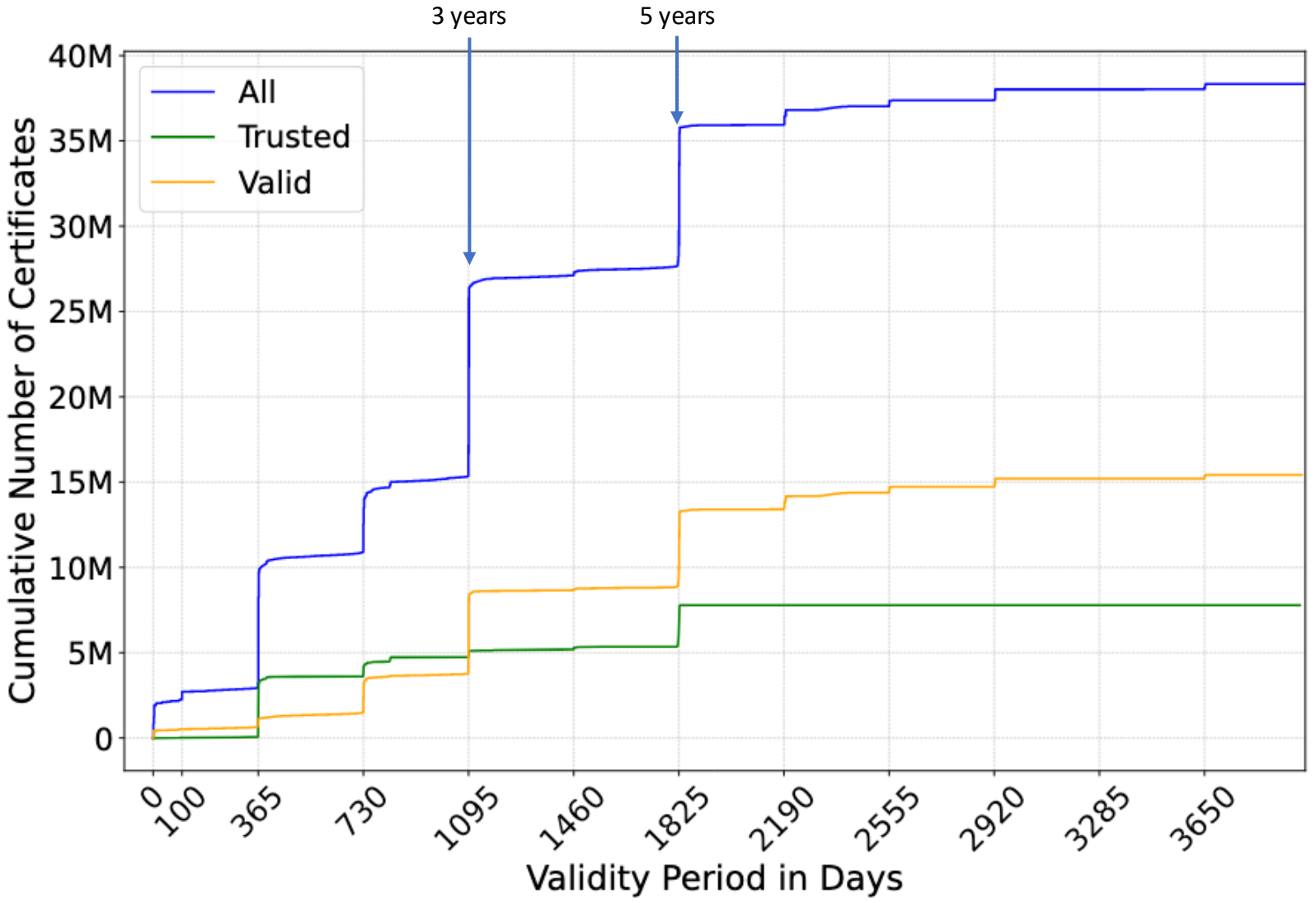
Certificate Authority	Number of Certificates (rounded)
UniTrust (CN)	3,300,000 (14%)
SK ID Solutions AS (EE)	2,900,000 (12%)
ArubaPEC S.p.A. (IT)	2,400,000 (10%)
D-Trust GmbH (DE)	2,200,000 (10%)
Digi- ja västo[...] (FI)	1,300,000 (6%)
A-Trust [...] (AT)	1,000,000 (4%)

Chain Validation Results

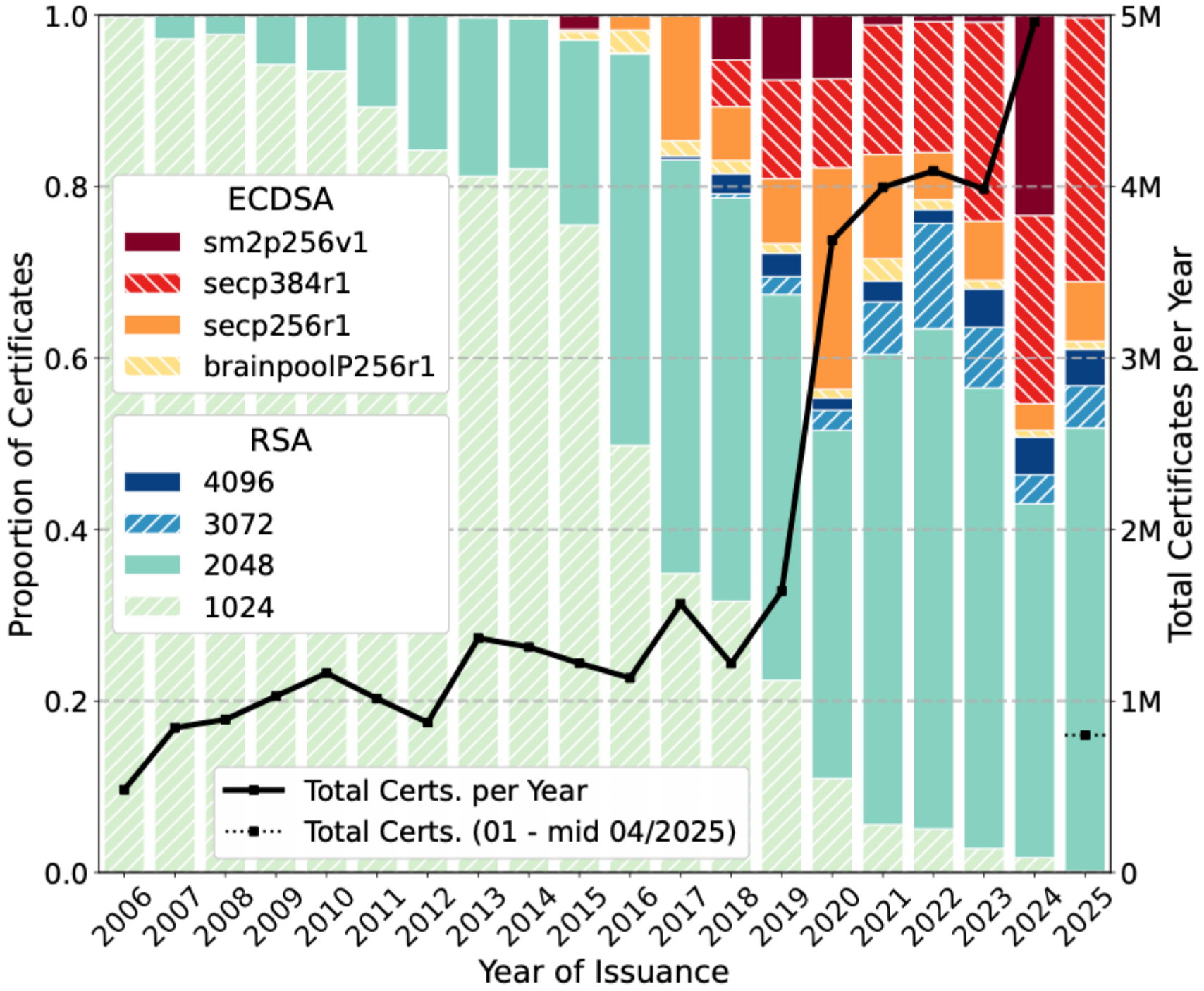
Trust Status	Expired	Valid	Total	Percentage
Total	25,000,000	13,000,000	38,000,000	100.0 %
Trusted	5,000,000	2,800,000	7,800,000	20.5 %
Untrusted	9,000,000	6,500,000	15,500,000	40.5 %
Non-Validatable	11,000,000	3,700,000	14,900,000	39.0 %




Validity Period of S/MIME Certificate



Algorithms


ECDSA
sm2p256v1
secp384r1
secp256r1
brainpoolP256r1
RSA
4096
3072
2048
1024
Total Certs. per Year
Total Certs. (01 - mid 04/2025)
Proportion of Certificates
Total Certificates per Year
Year of Issuance
0.0
0.2
0.4
0.6
0.8
1.0
0
1M
2M
3M
4M
5M
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025

Finding Weak Keys

$$N_1 = p * q$$
$$N_2 = p * r$$

Factoring (fastgcd, small/known Factors)

≈ 8.100 Certs.

"Public" private Keys

≈ 444 Certs.

Insecurely Generated

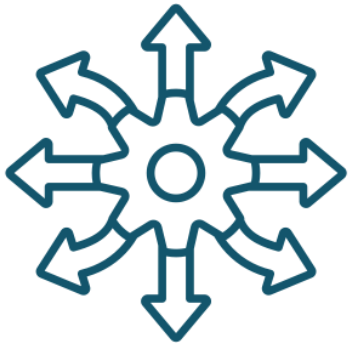
≈ 62.000 Certs.

Invalid Keys

≈ 500 Certs.

S/MIME Takeaways

- There are **a lot** of S/MIME capable certificates on the Internet
  - Email Clients will accept almost anything
  - Lots of them are concentrated on a few large CAs
- Generally, the S/MIME PKI is heading in the right direction:
  - Better algorithms (Small RSA ➔ ECC)
  - Few “insecure” keys
  - Baseline Requirements starting to take effect

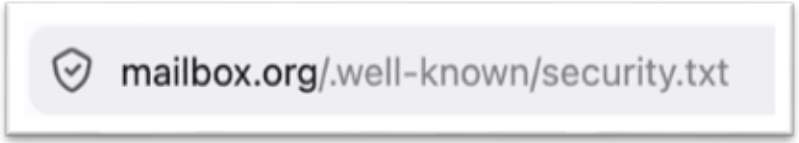


S/MIME Takeaways
What to do if you manage a (internal) PKI?

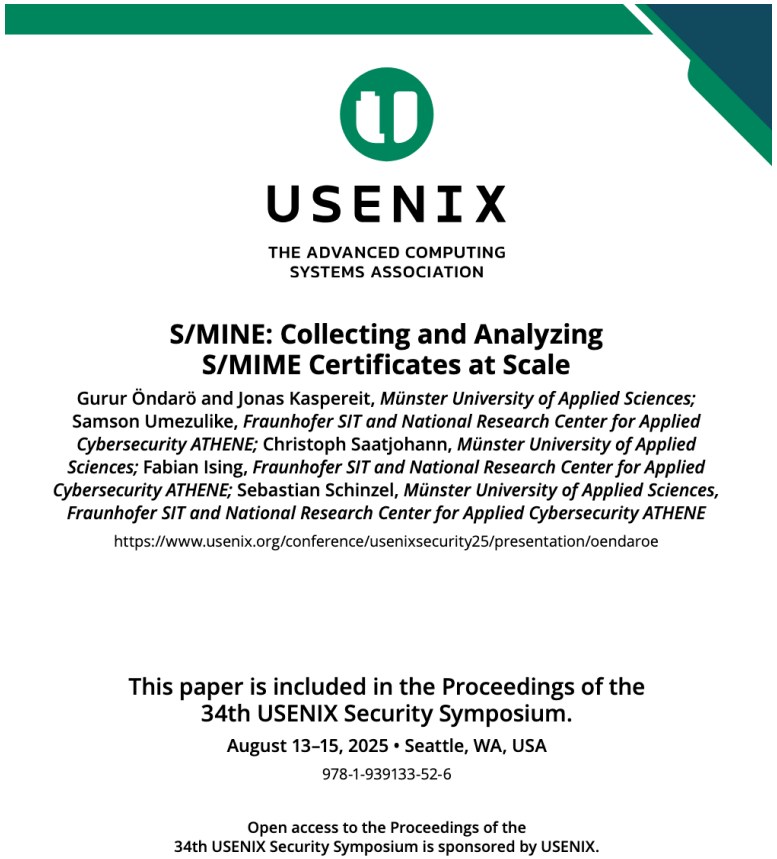
1. Adapt the most important rules of the Baseline Requirements
   - Validity Periods
   - Strong Keys and Algorithms
   - Certificate Linting
   - Check and maintain revocation infrastructure

2. Make sure that the Authority Information Access is correctly set

3. Make sure there is a way to reach you when researchers want to do so ;-)



Reference



USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

S/MINE: Collecting and Analyzing S/MIME Certificates at Scale

Gurur Öndarö and Jonas Kaspereit, *Münster University of Applied Sciences;* Samson Umezulike, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Christoph Saatjohann, *Münster University of Applied Sciences;* Fabian Ising, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Sebastian Schinzel, *Münster University of Applied Sciences, Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE*

https://www.usenix.org/conference/usenixsecurity25/presentation/oendaroe

This paper is included in the Proceedings of the 34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the 34th USENIX Security Symposium is sponsored by USENIX.

Gurur Öndarö[1,2], Jonas Kaspereit[1], Samson Umezulike[2], Christoph Saatjohann[1], Fabian Ising[2], and Sebastian Schinzel[1,2]

[1]Münster University of Applied Sciences
[2]Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE

Conclusion and Takeaways

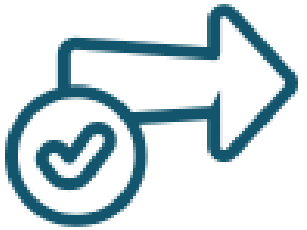
Conclusions

Securely running LDAP and S/MIME can be hard

Both are easy to “set and forget”

Security Hygiene!

Requirements are hard But: Improve security!



We are going the right way (for S/MIME)

Checklist: LDAP

- ❑ Is your LDAP server Internet reachable? (Does it need to be?)
- ❑ What attributes do you expose? (`ldapsearch -x -h <HOST>` / Some LDAP Browser)
  - ❑ Private Data?
  - ❑ Plaintext Passwords!?
- ❑ Is unauthenticated bind disabled?
- ❑ Is LDAPS (TCP/636) enabled/enforced? What about STARTTLS on 389?
- ❑ Is your TLS library up to date? (>= TLSv1.2, TLSv1.3 preferred)
- ❑ Are there known CVEs for your LDAP server?

Checklist: S/MIME (Internal PKI)

- ❑ Email addresses in the SAN?
- ❑ Validity periods <= 825 days?
- ❑ Strong algorithms used? (e.g., SHA-256+, RSA-2048+, ECC)
- ❑ Authority Information Access and Revocation:
  - ❑ Are CRL issuers set correctly?
  - ❑ Does OSCP or CRL (preferred) work?
  - ❑ Do you have a (automated) process for revoking certificates?
- ❑ Are you linting certificates before issuing?

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

Von Klartextpasswörtern und schwachen Schlüsseln: Eine Studie über LDAP-Server und ihre S/MIME-Zertifikate

Dr.-Ing. Fabian Ising [1, 2]
Gurur Öndarö, M. Sc.[1, 2, 3]

[1] Fraunhofer SIT
[2] ATHENE – Nationales Forschungszentrum für Angewandte Cybersicherheit
[3] FH Münster

SLAC 2026