Energy Community

BLUEPRINT ENERGY SOLUTIONS

The latest development in EU and new cybersecurity trends in energy

Blueprint Energy Solutions GmbH
Ferenc Suba, project lead expert

Vienna, 17.09.2019.

Agenda

1. Overall threat landscape in 2019
2. Grid related issues
3. Cybersecurity Act – ENISA in focus
4. ENISA activities regarding The Cybersecurity Act

Overal threat landcape in 2019

WORLD ECONOMIC FORUM - RISK SNAPSHOT: SMART GRIDS PAPER

„Worldwide spending on the IoT is forecast to reach $1.2 trillion in 2020 - more than half of what the world is forecast to spend on defence ($2 trillion) and more than double the spend on digital advertising ($500 billion). Utilities rank fourth among the industries spending the most on this technology - but without securing these new technologies, the risks may make people question whether they outweigh the benefits."

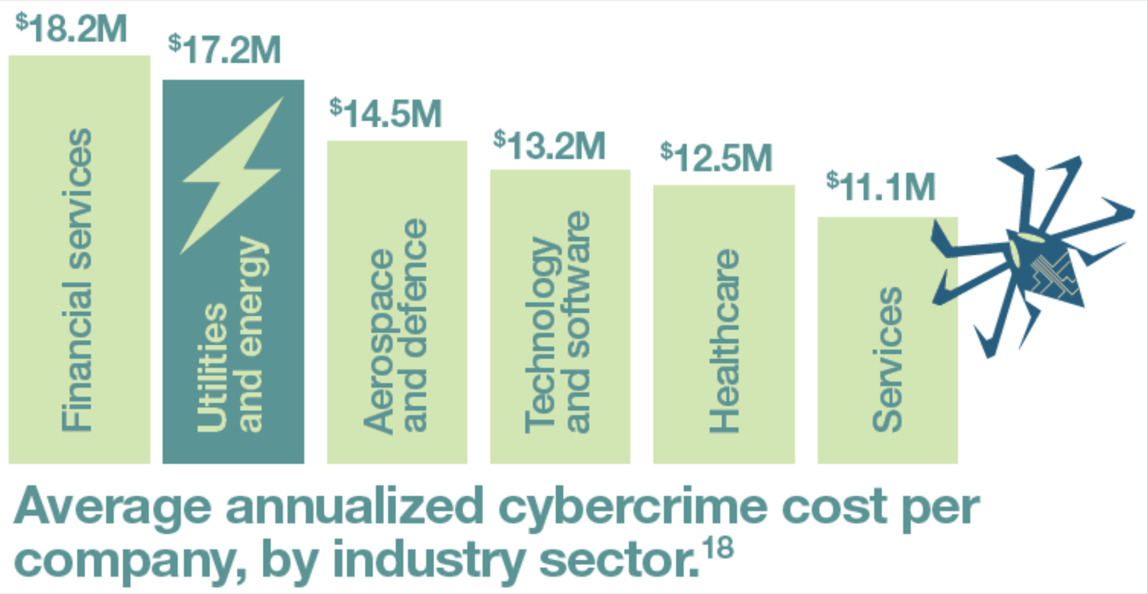
„The cost of a cyberattack on the US smart power grid is estimated to be $1 trillion – roughly eight times the cost of cleaning up the Fukushima nuclear disaster. „

https://www.weforum.org/reports/risk-snapshot-smart-grids

Overal threat landcape in 2019

WORLD ECONOMIC FORUM - RISK SNAPSHOT: SMART GRIDS PAR

A six-hour winter blackout in mainland France could result in damages totalling over €1.5 billion ($1.7 billion)[19]



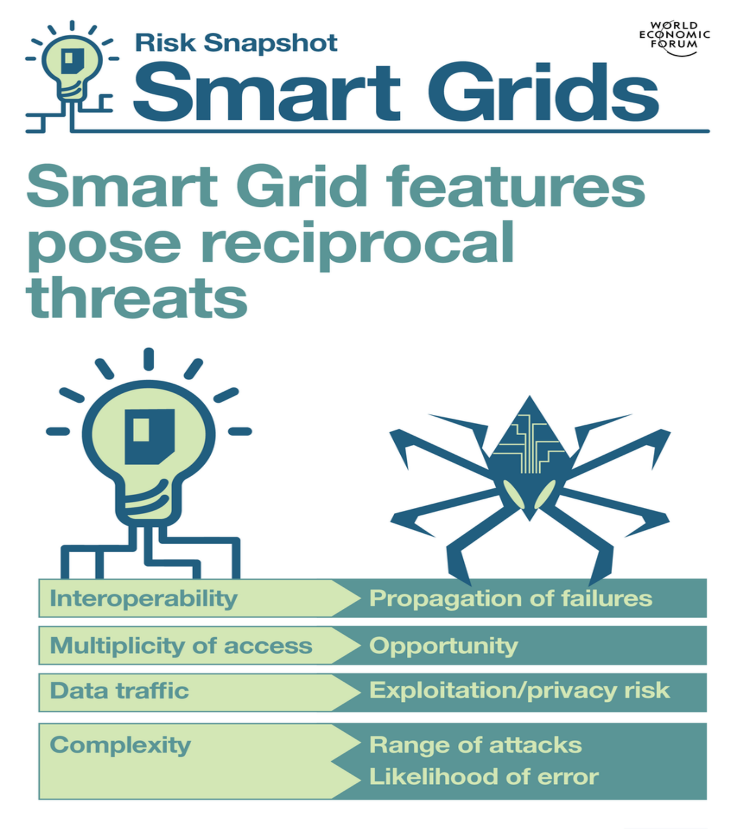
Average annualized cybercrime cost per company, by industry sector.[18]

https://www.weforum.org/reports/risk-snapshot-smart-grids

Be BLUEPRINT ENERGY SOLUTIONS

Overal threat landcape in 2019

WORLD ECONOMIC FORUM - RISK SNAPSHOT: SMART GRIDS PAPER



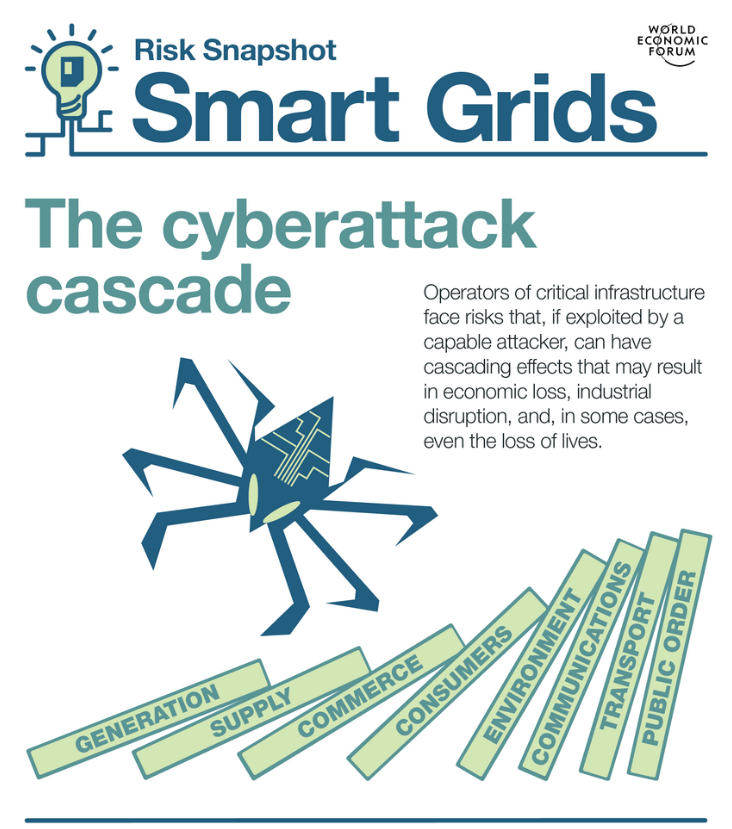
Risk Snapshot

WORLD ECONOMIC FORUM

Smart Grids

Smart Grid features pose reciprocal threats

Interoperability	Propagation of failures
Multiplicity of access	Opportunity
Data traffic	Exploitation/privacy risk
Complexity	Range of attacks Likelihood of error



Risk Snapshot

WORLD ECONOMIC FORUM

Smart Grids

The cyberattack cascade

Operators of critical infrastructure face risks that, if exploited by a capable attacker, can have cascading effects that may result in economic loss, industrial disruption, and, in some cases, even the loss of lives.

GENERATION
SUPPLY
COMMERCE
CONSUMERS
ENVIRONMENT
COMMUNICATIONS
TRANSPORT
PUBLIC ORDER

https://www.weforum.org/reports/risk-snapshot-smart-grids

U.S. GOVERNMENT MAKES SURPRISE MOVE TO SECURE POWER GRID FROM CYBERATTACKS

„The U.S. has responded with a new strategy: rather than bringing in new technology and skills, it will use analog and manual technology to isolate the grid's most important control systems. This, the government says, will limit the reach of a catastrophic outage."

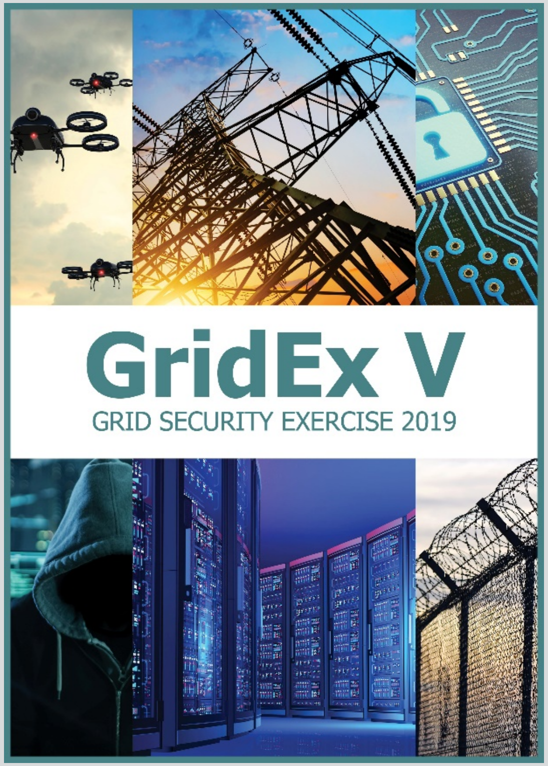
„The North American Electric Reliability Corporation (NERC) reports that a cyberattack on the US power grid earlier this year was caused by a target entity's network perimeter firewall flaw. NERC says attackers exploited a vulnerability in the web interface of a vendor firewall, enabling attackers to repeatedly reboot the devices and cause a denial-of-service condition. The unexpected reboots let to communication outages in firewalls that controlled communication between the control center and multiple remote generation sites, and between equipment on these sites. All firewalls were network perimeter devices."
Source: Dark Reading

Forbes – 3rd of July 2019
https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/

Grid related isuues in 2019

RISK FROM TECHNOLOGY

- ❑ Vendor based risk (zero-day threats, design flaw)
- ❑ Technology based risk (legacy systems, lack of patching)
- ❑ Process based risk (bad incident handling)
- ❑ Cascading risk (vertical and horizontal, cross-country)
- ❑ EMP/CMI risk!



NERC - US GridEx V

„GridEx V will be held November 13-14, 2019. The exercise is designed for distributed play, coordinated locally by a designated asset owner and operator lead planner. An executive tabletop exercise (TTX) occurs concurrently and includes senior industry and government leaders."

https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEx.aspx

Cybersecurity Act – ENISA in focus

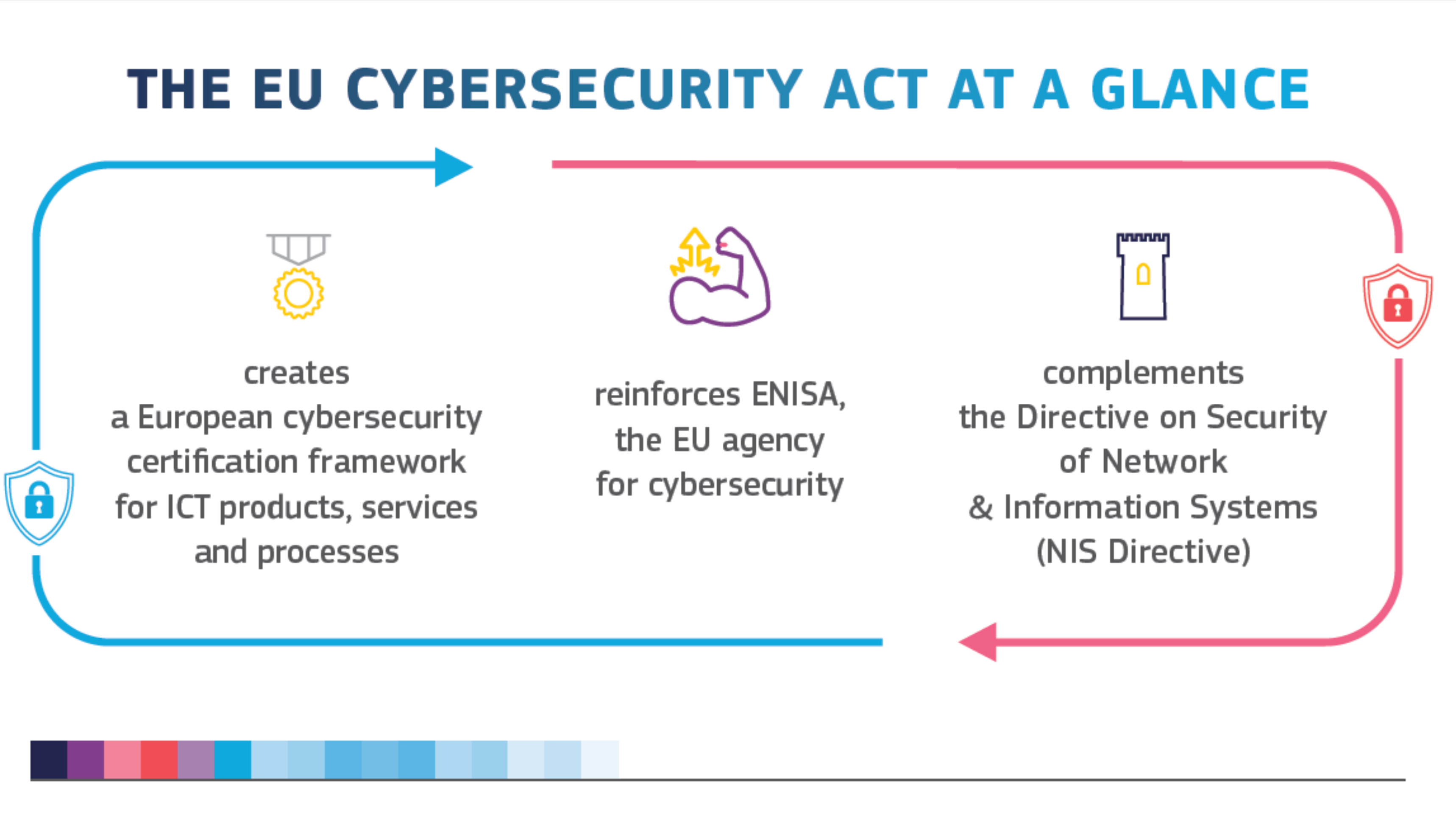
A NEW ERA DAWNS ON ENISA

❑ 7th June 2019, the EU Cybersecurity Act was published in the Official Journal of the European Union and came into force on 27th June 2019

❑ ENISA have a key role in setting up and maintaining the European cybersecurity certification framework (products, processes, services)

❑ ENISA is mandated to increase operational cooperation at EU level (national CSIRT secretariat,

Cybersecurity Act – ENISA in focus



THE EU CYBERSECURITY ACT AT A GLANCE

creates
a European cybersecurity
certification framework
for ICT products, services
and processes

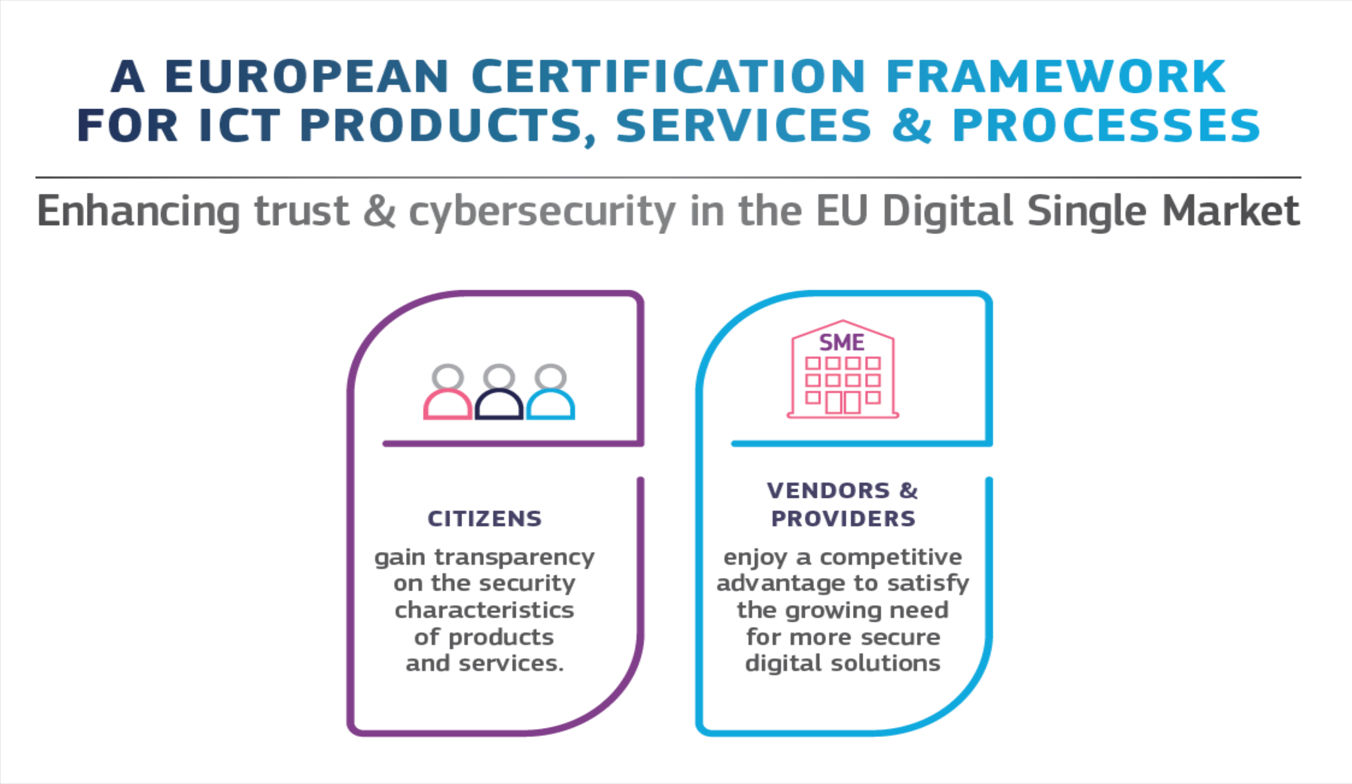
reinforces ENISA,
the EU agency
for cybersecurity

complements
the Directive on Security
of Network
& Information Systems
(NIS Directive)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

Cybersecurity Act – ENISA in focus

A NEW ERA DAWNS ON ENISA



A EUROPEAN CERTIFICATION FRAMEWORK FOR ICT PRODUCTS, SERVICES & PROCESSES

Enhancing trust & cybersecurity in the EU Digital Single Market

CITIZENS

gain transparency on the security characteristics of products and services.

VENDORS & PROVIDERS

enjoy a competitive advantage to satisfy the growing need for more secure digital solutions

Following the entry into force of the Cybersecurity Act on 27 June 2019, the European Commission has requested ENISA to prepare a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS Mutual Recognition Agreement.

https://www.enisa.europa.eu/news/enisa-news/call-for-expression-of-interest-for-the-first-ad-hoc-working-group-on-cybersecurity-certification

ENISA activities regarding The Cybersecurity Act

A NEW ERA DAWNS ON ENISA

- ❑ 4th September 2019, ENISA publishes a report to guide incident response teams forming a community to choose secure communications solutions.
- ❑ The methodology presented could also be valid for other operational teams grouped in an information sharing and analysis centre (EE-ISAC)
- ❑ ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination

https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

As of July 2019 there are more than 414 incident response teams in Europe.

This project on secure communication solutions has been conducted with a specific community and scenario in mind. This community could be a group of incident response teams forming a decentral community or an operational community grouped in an information sharing and analysis centre (ISAC).

This model is that a community already have in place chat, encrypted email and a shared secure space on the web, where to share information.

EE-ISAC

CSIRTs NETWORK

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

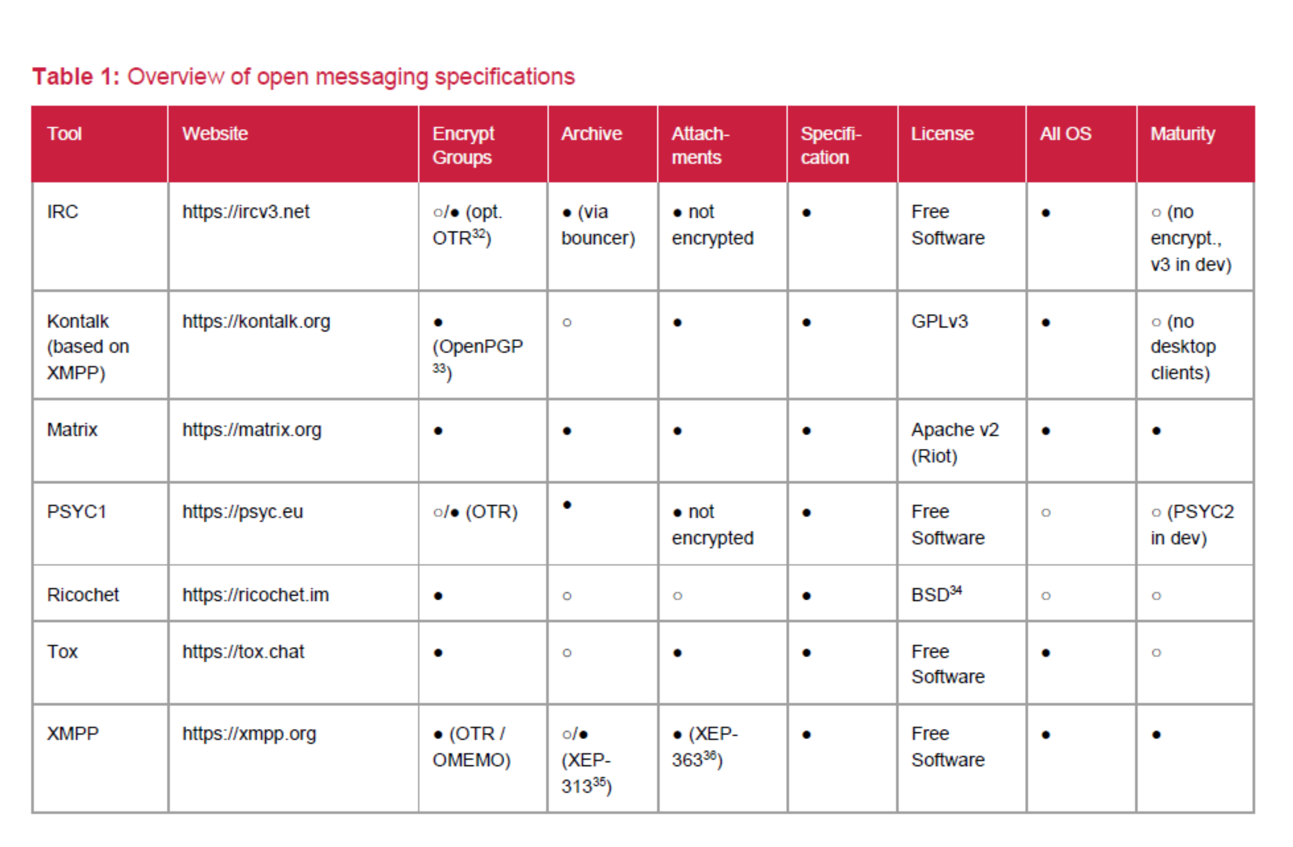


Table 1: Overview of open messaging specifications

Tool	Website	Encrypt Groups	Archive	Attachments	Specification	License	All OS	Maturity
IRC	https://ircv3.net	○/● (opt. OTR[32])	● (via bouncer)	● not encrypted	●	Free Software	●	○ (no encrypt., v3 in dev)
Kontalk (based on XMPP)	https://kontalk.org	● (OpenPGP [33])	○	●	●	GPLv3	●	○ (no desktop clients)
Matrix	https://matrix.org	●	●	●	●	Apache v2 (Riot)	●	●
PSYC1	https://psyc.eu	○/● (OTR)	●	● not encrypted	●	Free Software	○	○ (PSYC2 in dev)
Ricochet	https://ricochet.im	●	○	○	●	BSD[34]	○	○
Tox	https://tox.chat	●	○	●	●	Free Software	●	○
XMPP	https://xmpp.org	● (OTR / OMEMO)	○/● (XEP-313[35])	● (XEP-363[36])	●	Free Software	●	●

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

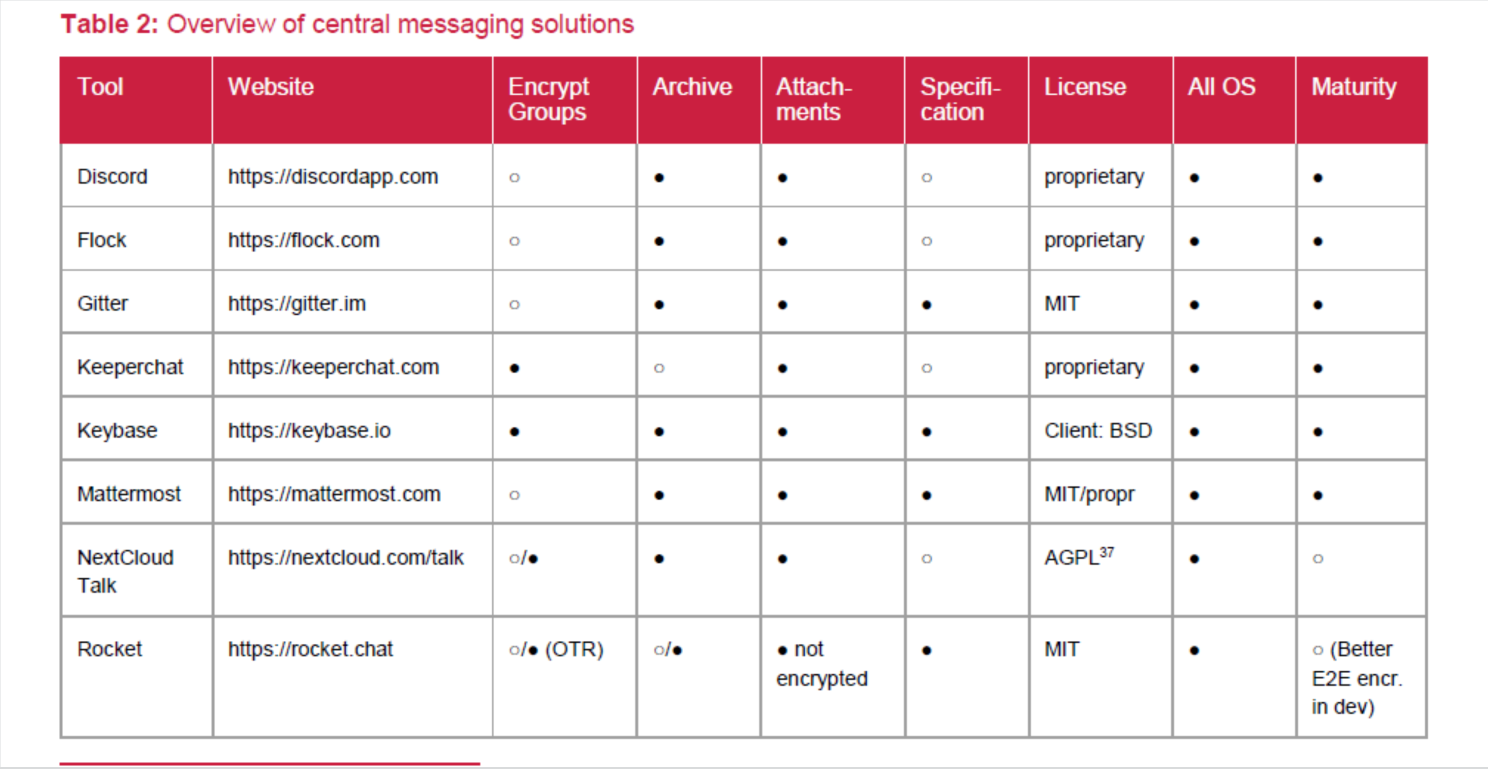


Table 2: Overview of central messaging solutions

Tool	Website	Encrypt Groups	Archive	Attach-ments	Specifi-cation	License	All OS	Maturity
Discord	https://discordapp.com	○	●	●	○	proprietary	●	●
Flock	https://flock.com	○	●	●	○	proprietary	●	●
Gitter	https://gitter.im	○	●	●	●	MIT	●	●
Keeperchat	https://keeperchat.com	●	○	●	○	proprietary	●	●
Keybase	https://keybase.io	●	●	●	●	Client: BSD	●	●
Mattermost	https://mattermost.com	○	●	●	●	MIT/propr	●	●
NextCloud Talk	https://nextcloud.com/talk	○/●	●	●	○	AGPL[37]	●	○
Rocket	https://rocket.chat	○/● (OTR)	○/●	● not encrypted	●	MIT	●	○ (Better E2E encr. in dev)

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

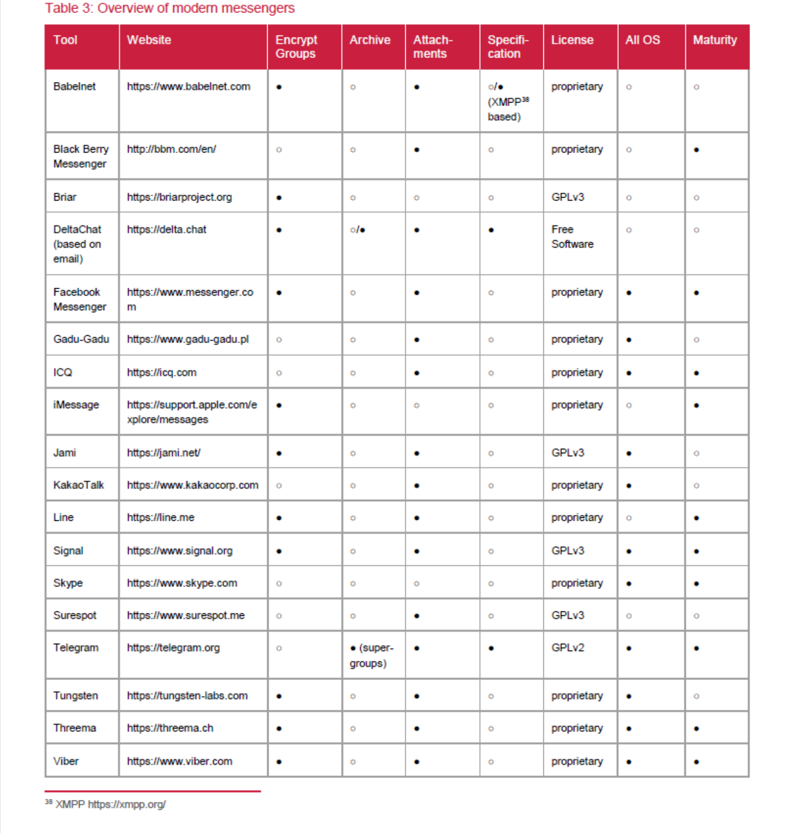


Table 3: Overview of modern messengers

Tool	Website	Encrypt Groups	Archive	Attach-ments	Specifi-cation	License	All OS	Maturity
Babelnet	https://www.babelnet.com	●	○	●	○/● (XMPP[38] based)	proprietary	○	○
Black Berry Messenger	http://bbm.com/en/	○	○	●	○	proprietary	○	●
Briar	https://briarproject.org	●	○	○	○	GPLv3	○	○
DeltaChat (based on email)	https://delta.chat	●	○/●	●	●	Free Software	○	○
Facebook Messenger	https://www.messenger.com	●	○	●	○	proprietary	●	●
Gadu-Gadu	https://www.gadu-gadu.pl	○	○	●	○	proprietary	●	○
ICQ	https://icq.com	○	○	●	○	proprietary	●	●
iMessage	https://support.apple.com/explore/messages	●	○	○	○	proprietary	○	●
Jami	https://jami.net/	●	○	●	○	GPLv3	●	○
KakaoTalk	https://www.kakaocorp.com	○	○	●	○	proprietary	●	○
Line	https://line.me	●	○	●	○	proprietary	○	●
Signal	https://www.signal.org	●	○	●	○	GPLv3	●	●
Skype	https://www.skype.com	○	○	○	○	proprietary	●	●
Surespot	https://www.surespot.me	○	○	●	○	GPLv3	○	○
Telegram	https://telegram.org	○	● (super-groups)	●	●	GPLv2	●	●
Tungsten	https://tungsten-labs.com	●	○	●	○	proprietary	●	○
Threema	https://threema.ch	●	○	●	○	proprietary	●	●
Viber	https://www.viber.com	●	○	●	○	proprietary	●	●

[38] XMPP https://xmpp.org/

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

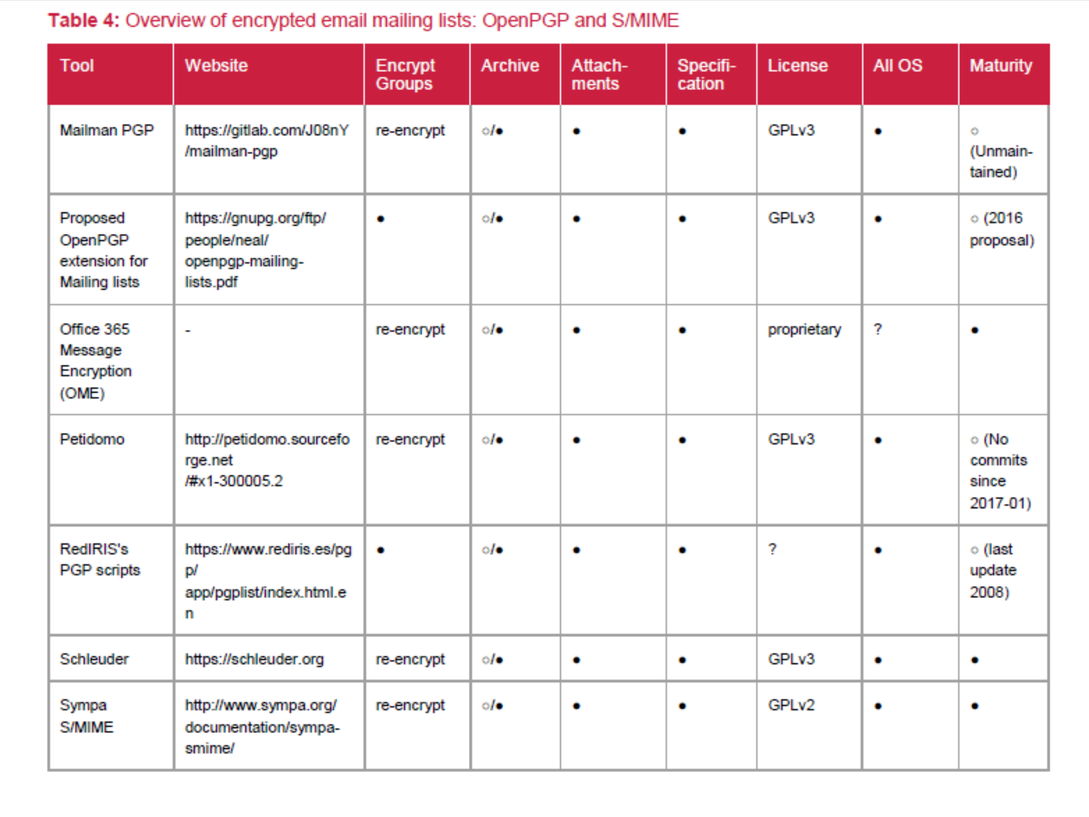


Table 4: Overview of encrypted email mailing lists: OpenPGP and S/MIME

Tool	Website	Encrypt Groups	Archive	Attach-ments	Specifi-cation	License	All OS	Maturity
Mailman PGP	https://gitlab.com/J08nY/mailman-pgp	re-encrypt	○/●	●	●	GPLv3	●	○ (Unmain-tained)
Proposed OpenPGP extension for Mailing lists	https://gnupg.org/ftp/people/neal/openpgp-mailing-lists.pdf	●	○/●	●	●	GPLv3	●	○ (2016 proposal)
Office 365 Message Encryption (OME)	-	re-encrypt	○/●	●	●	proprietary	?	●
Petidomo	http://petidomo.sourceforge.net /#x1-300005.2	re-encrypt	○/●	●	●	GPLv3	●	○ (No commits since 2017-01)
RedIRIS's PGP scripts	https://www.rediris.es/pgp/ app/pgplist/index.html.en	●	○/●	●	●	?	●	○ (last update 2008)
Schleuder	https://schleuder.org	re-encrypt	○/●	●	●	GPLv3	●	●
Sympa S/MIME	http://www.sympa.org/documentation/sympa-smime/	re-encrypt	○/●	●	●	GPLv2	●	●

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

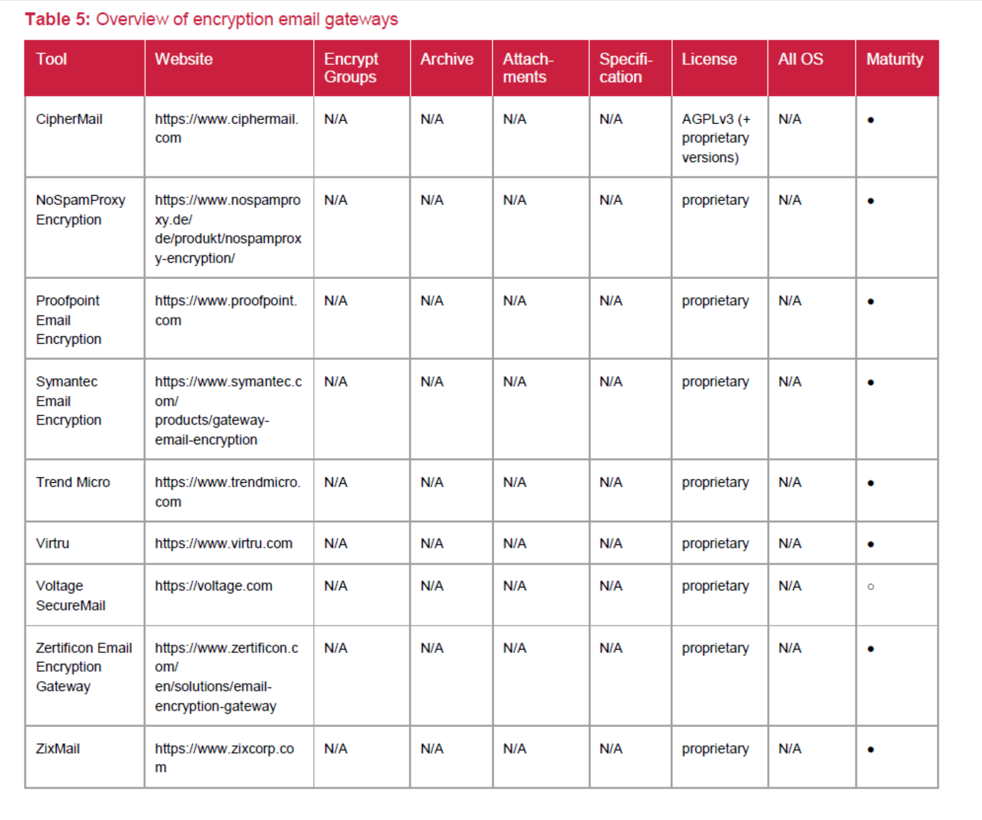


Table 5: Overview of encryption email gateways

Tool	Website	Encrypt Groups	Archive	Attachments	Specification	License	All OS	Maturity
CipherMail	https://www.ciphermail.com	N/A	N/A	N/A	N/A	AGPLv3 (+ proprietary versions)	N/A	●
NoSpamProxy Encryption	https://www.nospamproxy.de/de/produkt/nospamproxy-encryption/	N/A	N/A	N/A	N/A	proprietary	N/A	●
Proofpoint Email Encryption	https://www.proofpoint.com	N/A	N/A	N/A	N/A	proprietary	N/A	●
Symantec Email Encryption	https://www.symantec.com/products/gateway-email-encryption	N/A	N/A	N/A	N/A	proprietary	N/A	●
Trend Micro	https://www.trendmicro.com	N/A	N/A	N/A	N/A	proprietary	N/A	●
Virtru	https://www.virtru.com	N/A	N/A	N/A	N/A	proprietary	N/A	●
Voltage SecureMail	https://voltage.com	N/A	N/A	N/A	N/A	proprietary	N/A	○
Zertificon Email Encryption Gateway	https://www.zertificon.com/en/solutions/email-encryption-gateway	N/A	N/A	N/A	N/A	proprietary	N/A	●
ZixMail	https://www.zixcorp.com	N/A	N/A	N/A	N/A	proprietary	N/A	●

ENISA activities regarding The Cybersecurity Act

SECURE GROUP COMMUNICATIONS FOR INCIDENT RESPONSE AND OPERATIONAL COMMUNITIES

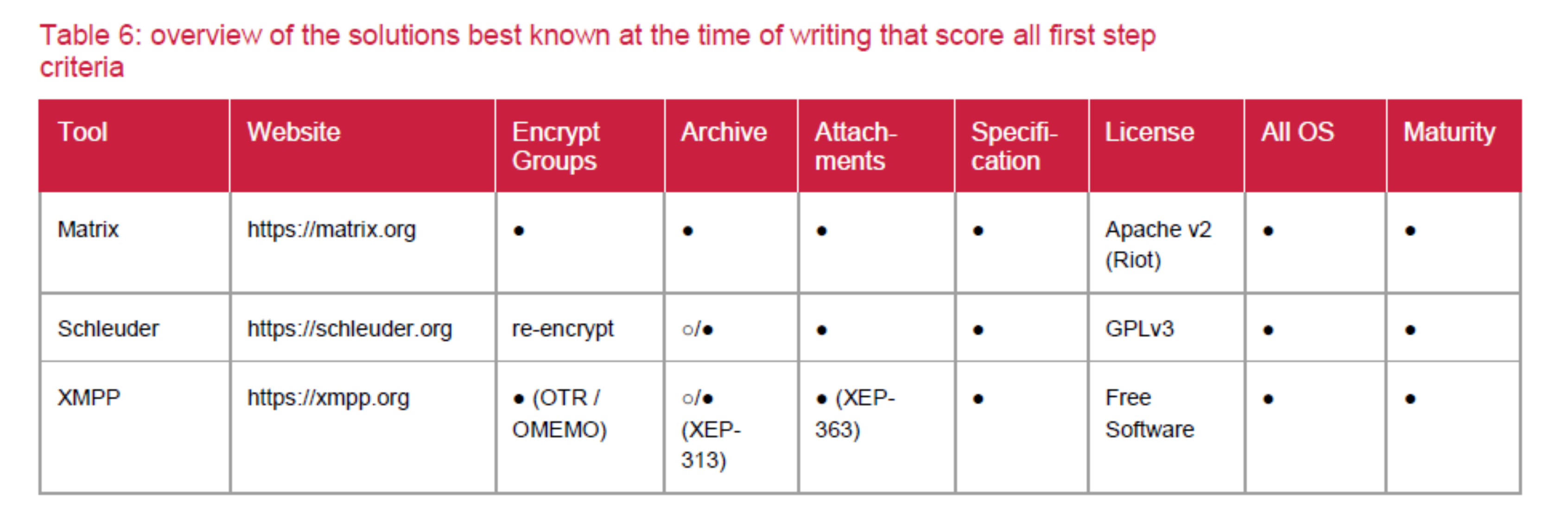


Table 6: overview of the solutions best known at the time of writing that score all first step criteria

Tool	Website	Encrypt Groups	Archive	Attach-ments	Specifi-cation	License	All OS	Maturity
Matrix	https://matrix.org	•	•	•	•	Apache v2 (Riot)	•	•
Schleuder	https://schleuder.org	re-encrypt	○/•	•	•	GPLv3	•	•
XMPP	https://xmpp.org	• (OTR / OMEMO)	○/• (XEP-313)	• (XEP-363)	•	Free Software	•	•

Questions?