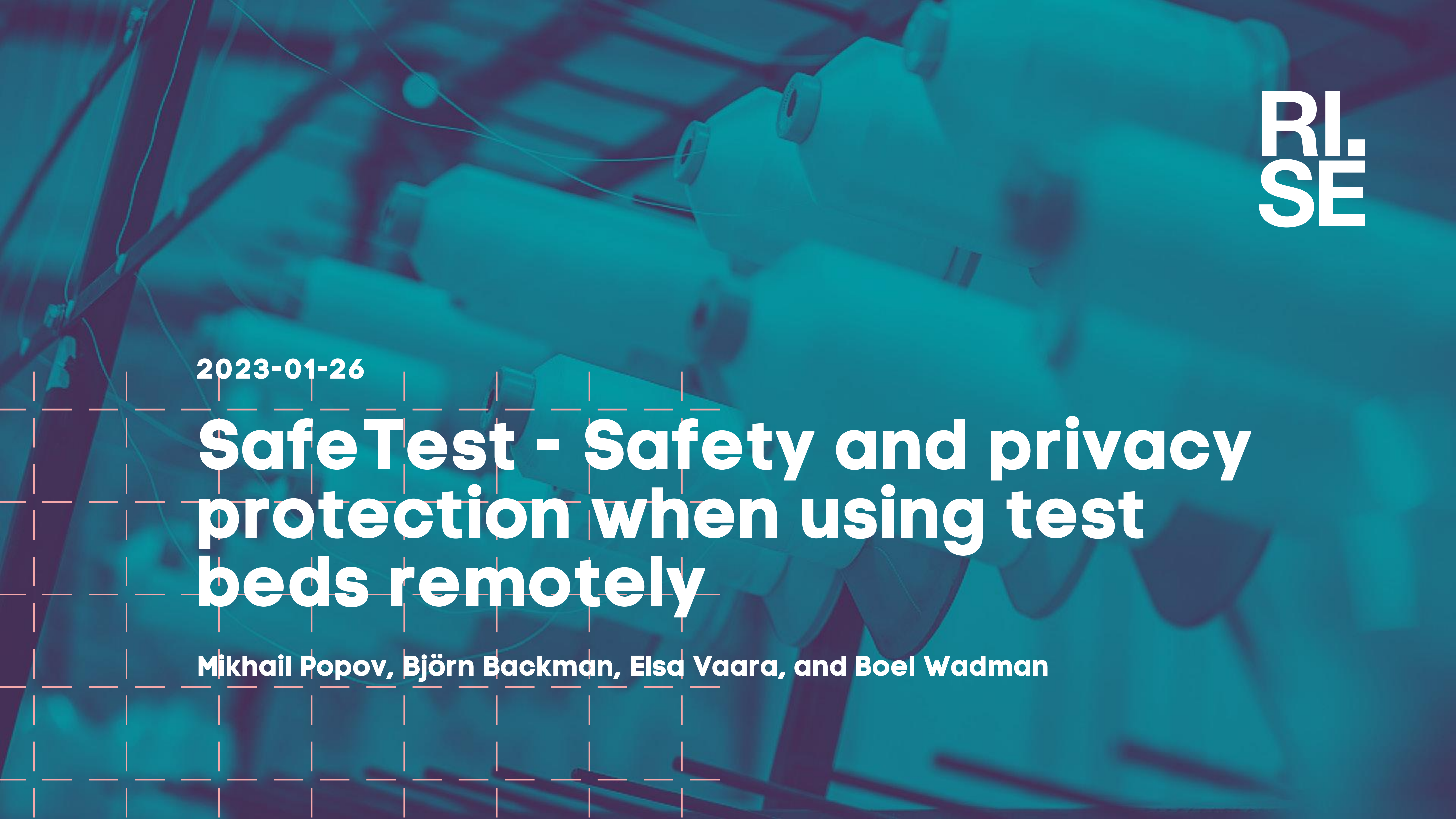


2023-01-26

SafeTest - Safety and privacy protection when using test beds remotely

Mikhail Popov, Björn Backman, Elsa Vaara, and Boel Wadman

Safetest

Safety and privacy protection when using test beds remotely

Vinnova project Aug 2021 – March 2023

Partners: **RISE**, **Prindit AB, AP&T**

- How to securely exchange data and run demonstrations from remote testbeds. (AP&T + RISE)
- How to ensure integrity for customers (Prindit)

VINNOVA Sweden's Innovation Agency · Prindit · AP&T AUTOMATION · PRESSES · TOOLING · RI. SE

Not-to-scale pictures from https://thesolarsystem.fandom.com/wiki/

Background

The problem is only partially technical.

Managing information in an organization:

- Expectation: information- and cybersecurity-centric
- Reality: user-centric

Improve scalability for security routines:

- Right language, volume & place

VINNOVA
Sweden's Innovation Agency

Prindit

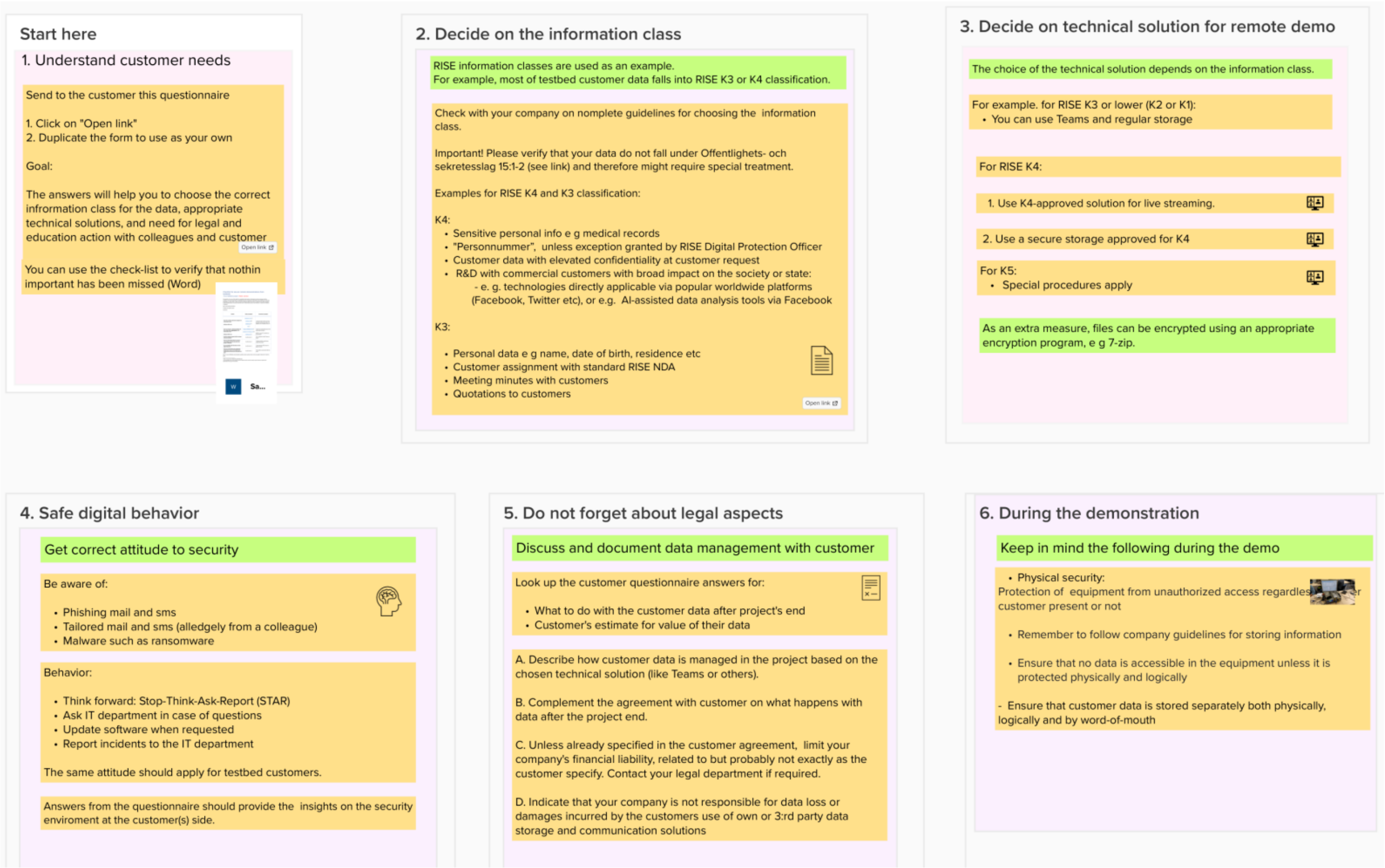
AP&T
AUTOMATION · PRESSES · TOOLING

RI.
SE

Not-to-scale pictures are from https://thesolarsystem.fandom.com/wiki/

Safetest easy-guide (lathund)

-for remote demonstrations



Start here

1. Understand customer needs

Send to the customer this questionnaire

1. Click on "Open link"
2. Duplicate the form to use as your own

Goal:

The answers will help you to choose the correct information class for the data, appropriate technical solutions, and need for legal and education action with colleagues and customer

You can use the check-list to verify that nothin important has been missed (Word)

2. Decide on the information class

RISE information classes are used as an example.
For example, most of testbed customer data falls into RISE K3 or K4 classification.

Check with your company on nomplete guidelines for choosing the information class.

Important! Please verify that your data do not fall under Offentlighets- och sekretesslag 15:1-2 (see link) and therefore might require special treatment.

Examples for RISE K4 and K3 classification:

K4:

- Sensitive personal info e g medical records
- "Personnummer", unless exception granted by RISE Digital Protection Officer
- Customer data with elevated confidentiality at customer request
- R&D with commercial customers with broad impact on the society or state:
  - e. g. technologies directly applicable via popular worldwide platforms (Facebook, Twitter etc), or e.g. AI-assisted data analysis tools via Facebook

K3:

- Personal data e g name, date of birth, residence etc
- Customer assignment with standard RISE NDA
- Meeting minutes with customers
- Quotations to customers

3. Decide on technical solution for remote demo

The choice of the technical solution depends on the information class.

For example. for RISE K3 or lower (K2 or K1):
- You can use Teams and regular storage

For RISE K4:

1. Use K4-approved solution for live streaming.

2. Use a secure storage approved for K4

For K5:
- Special procedures apply

As an extra measure, files can be encrypted using an appropriate encryption program, e g 7-zip.

4. Safe digital behavior

Get correct attitude to security

Be aware of:

- Phishing mail and sms
- Tailored mail and sms (alledgely from a colleague)
- Malware such as ransomware

Behavior:

- Think forward: Stop-Think-Ask-Report (STAR)
- Ask IT department in case of questions
- Update software when requested
- Report incidents to the IT department

The same attitude should apply for testbed customers.

Answers from the questionnaire should provide the insights on the security enviroment at the customer(s) side.

5. Do not forget about legal aspects

Discuss and document data management with customer

Look up the customer questionnaire answers for:

- What to do with the customer data after project's end
- Customer's estimate for value of their data

A. Describe how customer data is managed in the project based on the chosen technical solution (like Teams or others).

B. Complement the agreement with customer on what happens with data after the project end.

C. Unless already specified in the customer agreement, limit your company's financial liability, related to but probably not exactly as the customer specify. Contact your legal department if required.

D. Indicate that your company is not responsible for data loss or damages incurred by the customers use of own or 3:rd party data storage and communication solutions

6. During the demonstration

Keep in mind the following during the demo

- Physical security:

Protection of equipment from unauthorized access regardles er customer present or not

- Remember to follow company guidelines for storing information

- Ensure that no data is accessible in the equipment unless it is protected physically and logically

- Ensure that customer data is stored separately both physically, logically and by word-of-mouth

Shortlist of key steps

1. Understand customer needs and attitude to information security:
   - Questionnaire, part of the guide
2. Decide on information class (e g K1 - K5)
3. Decide on a technical solution for remote demo, depending on information class
4. Safe digital behavior: get correct attitude to security
5. Legal aspects: what happens with data under and after the project
6. During the demonstration: physical security etc.

Check-list is enclosed to the guide and mandatory - to not forget the key steps above.

VINNOVA Sweden's Innovation Agency
Prindit
AP&T AUTOMATION·PRESSES·TOOLING
RI. SE

Other things to think about

“Security is only as strong as the weakest link”

- Reach and scalability of security routines is key:
  - Use right language, right volume, and right place
  - Make information classification easy and solutions available
  - Same attitude applies to the customer side
- Right tool for right information class
- Pen-test the technical solution for higher info classes, if open source.

Public version of “lathund”/easy-guide available soon

Mikhail Popov

mikhail.popov@ri.se

Elsa Vaara

elsa.vaara@ri.se

Boel Wadman

boel.wadman@ri.se