PROTECTION POKER - A GAME FOR RISK ESTIMATION

Martin Gilje Jaatun (Yaw-toon)

Martin.G.Jaatun@sintef.no @seniorfrosk

Based on the original game by Laurie Williams, NCSU

Efficient and effective software security = risk based software security

SoS-Agile

- Impossible to prevent all security flaws and vulnerabilities
  - Limited resources – time, money, expertise
- Most important to prevent, detect and remove flaws and vulnerabilities with high risk:
  - Can easily be exploited by attackers
  - May impact important assets

What is Protection Poker?

SoS-Agile

- Risk estimation in agile development teams
  - Originally by Laurie Williams, NCSU
  - Based on Planning Poker (effort estimation)

NC STATE UNIVERSITY

- Performed in the beginning of every iteration, by the full team
- Goal: Rank the security risk of the features to be implemented in the iteration
  - Ensure common understanding in the team on the need for security in this iteration – and in general

Risk = value x exposure

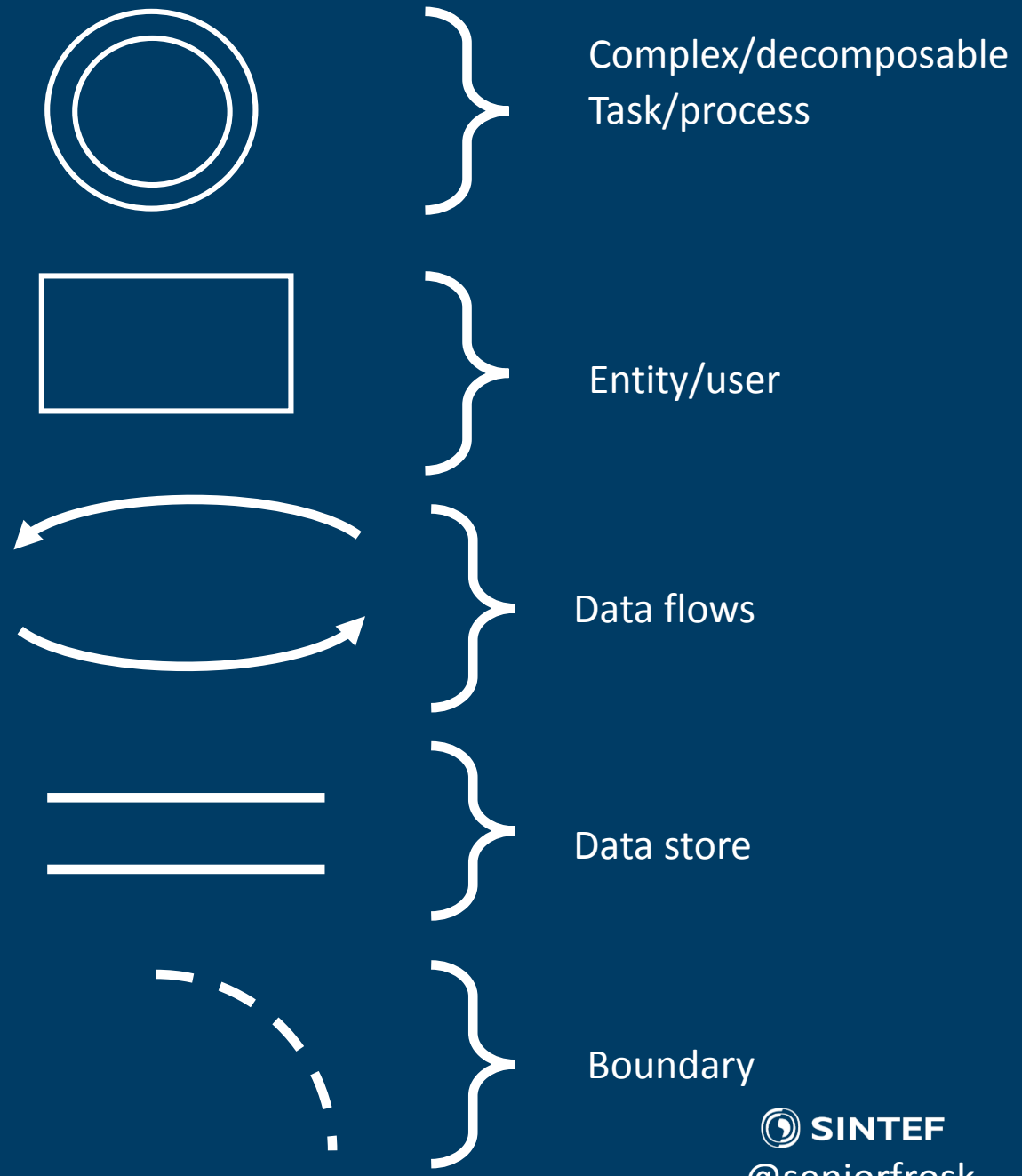
		Exposure	
		Hard to exploit	Easy to exploit
Asset	High value		High priority
	Low value	Low priority	

- **Exposure:**
  - Does it increase the attack surface?
  - What competence is needed to exploit this functionality?
  - What type of access to assets can be achieved (confidentiality, integrity, availability)?
- **Value of assets:**
  - What data is "touched upon" by the functionality?
  - Value of the assets for the organisation/customers/users?
  - Value for an attacker?

risk = (the total value of all assets that could be exploited with a successful attack) × (the exposure)

Interlude:
Data Flow Diagrams

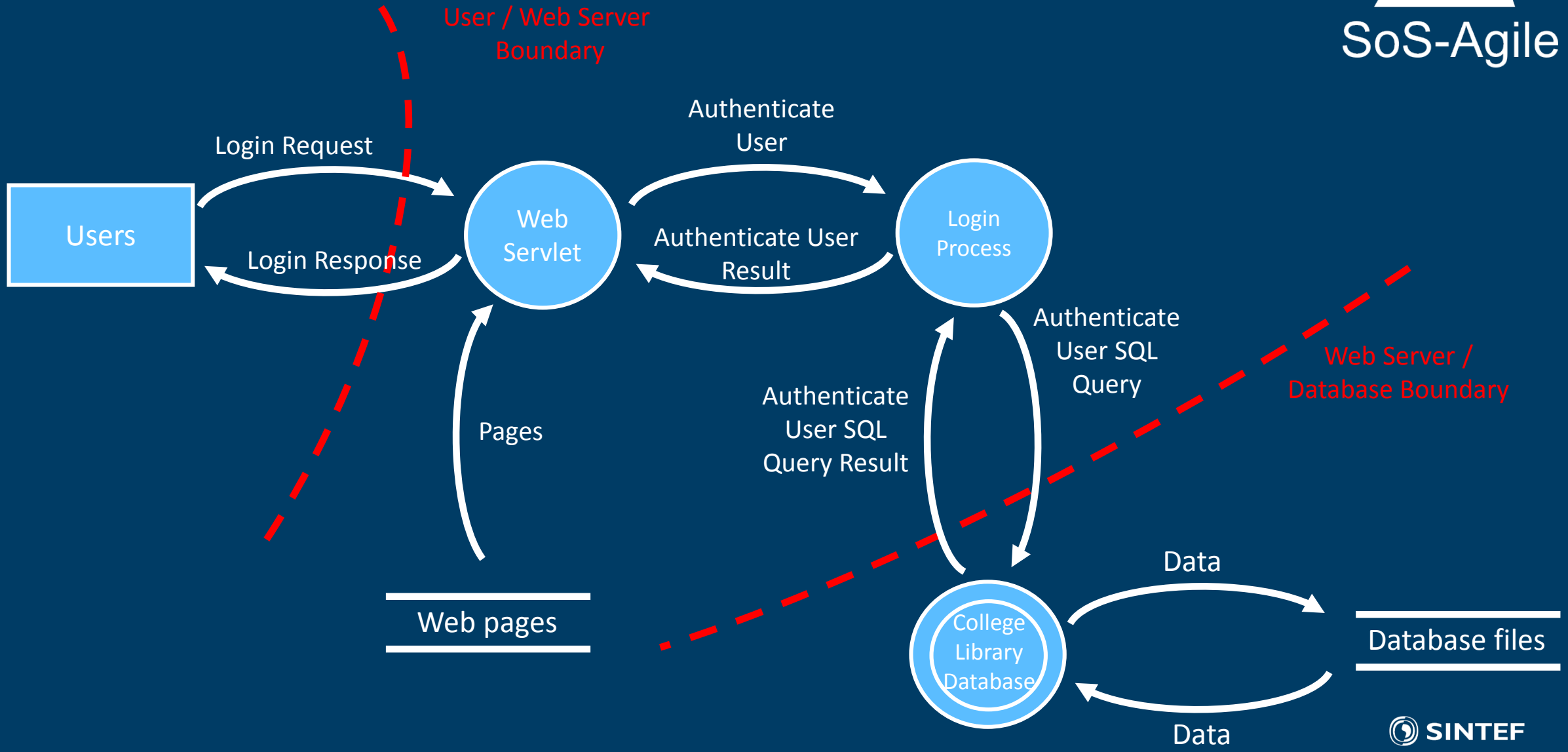
- Useful to get overview
- To understand the system's attack surface
  - Trust boundaries
  - How data flows in the system



SINTEF

@seniorfrosk

High-level description – A college library site



Case and data flow diagram inspired by https://www.owasp.org/index.php/Application_Threat_Modeling

SINTEF
@seniorfrosk

Example of new feature

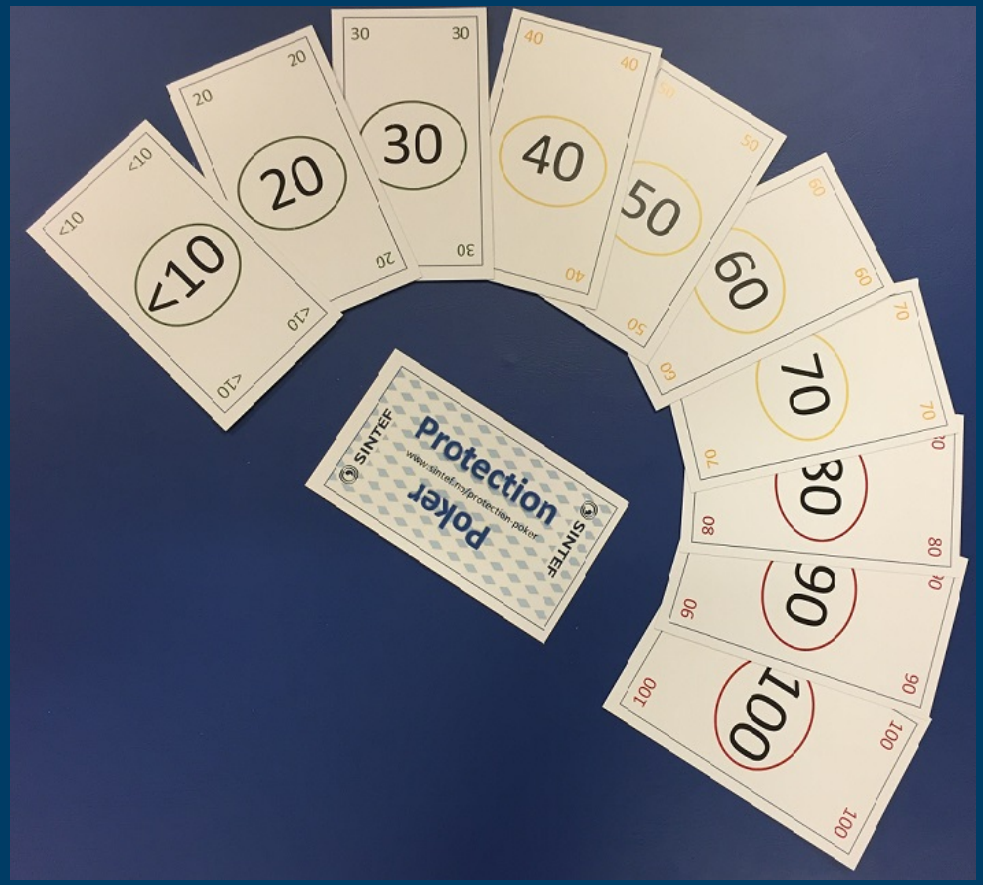
SoS-Agile

- *The students can make a request for a new book*
- Assets (just a few examples!)
  - Authentication credentials (login details)
  - Personal data
  - Webpages
  - Login session
  - Audit data
  - SQL queries
  - …
- NB: If you have many small features, consider grouping them (e.g. as use cases)

We play (at least) two rounds

- Value
  - For every *asset* the feature/requirement "touches"
- Exposure

NB: Consensus!



SoS-Agile

SINTEF

@seniorfrosk

First: Value of asset "Authentication credentials"

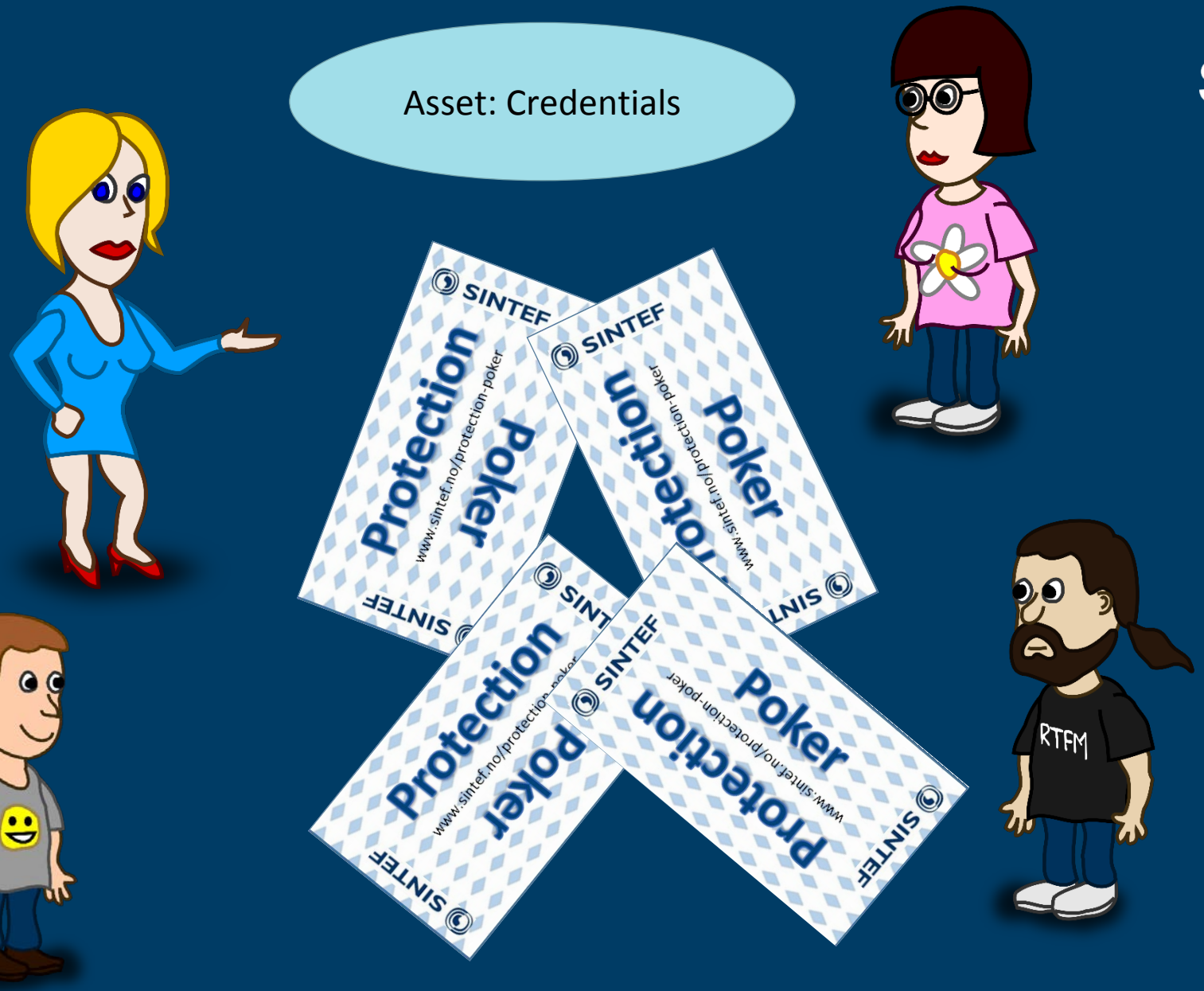
SoS-Agile

SINTEF

@seniorfrosk

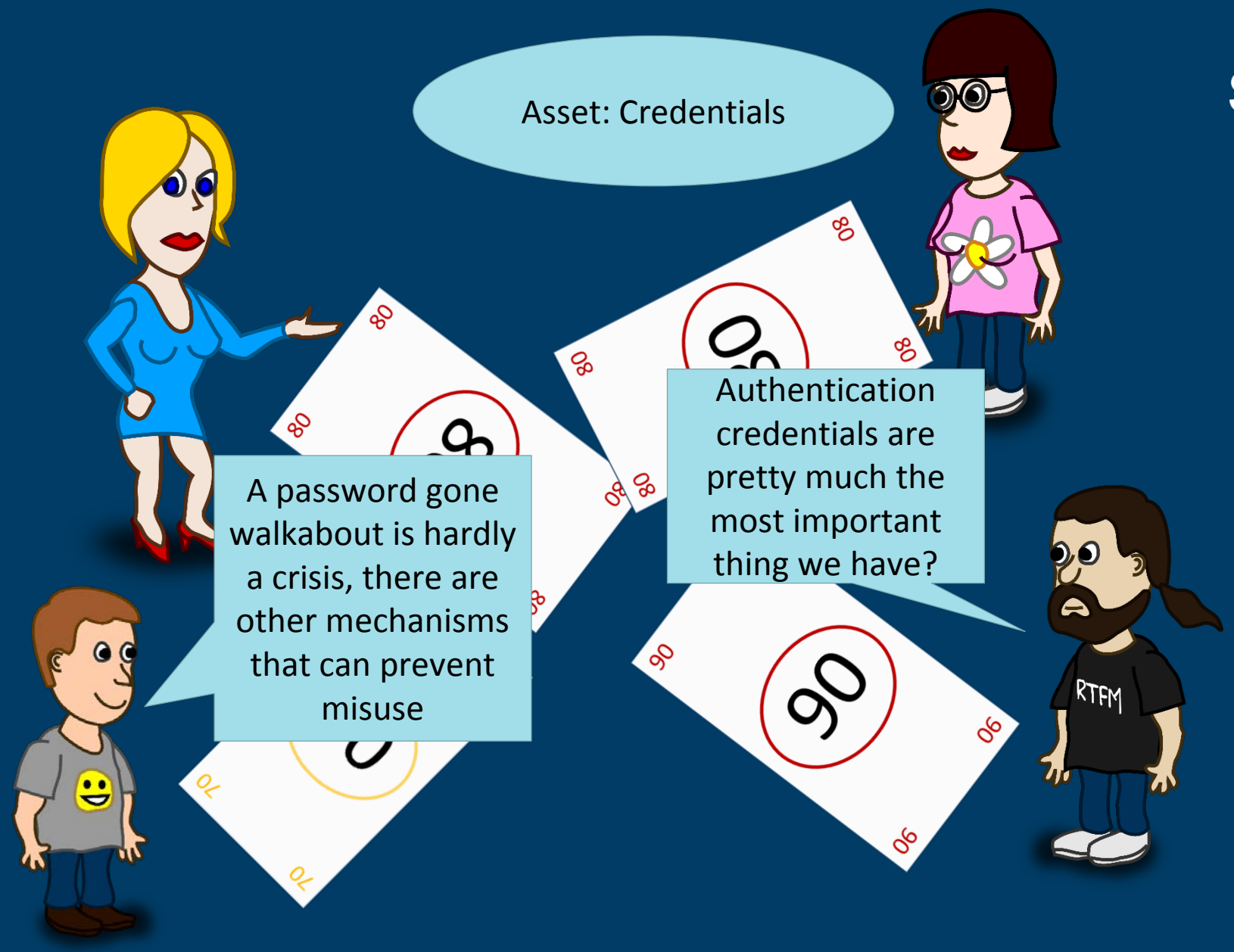
Let the game begin!

SoS-Agile



SINTEF
@seniorfrosk

Show your hand!



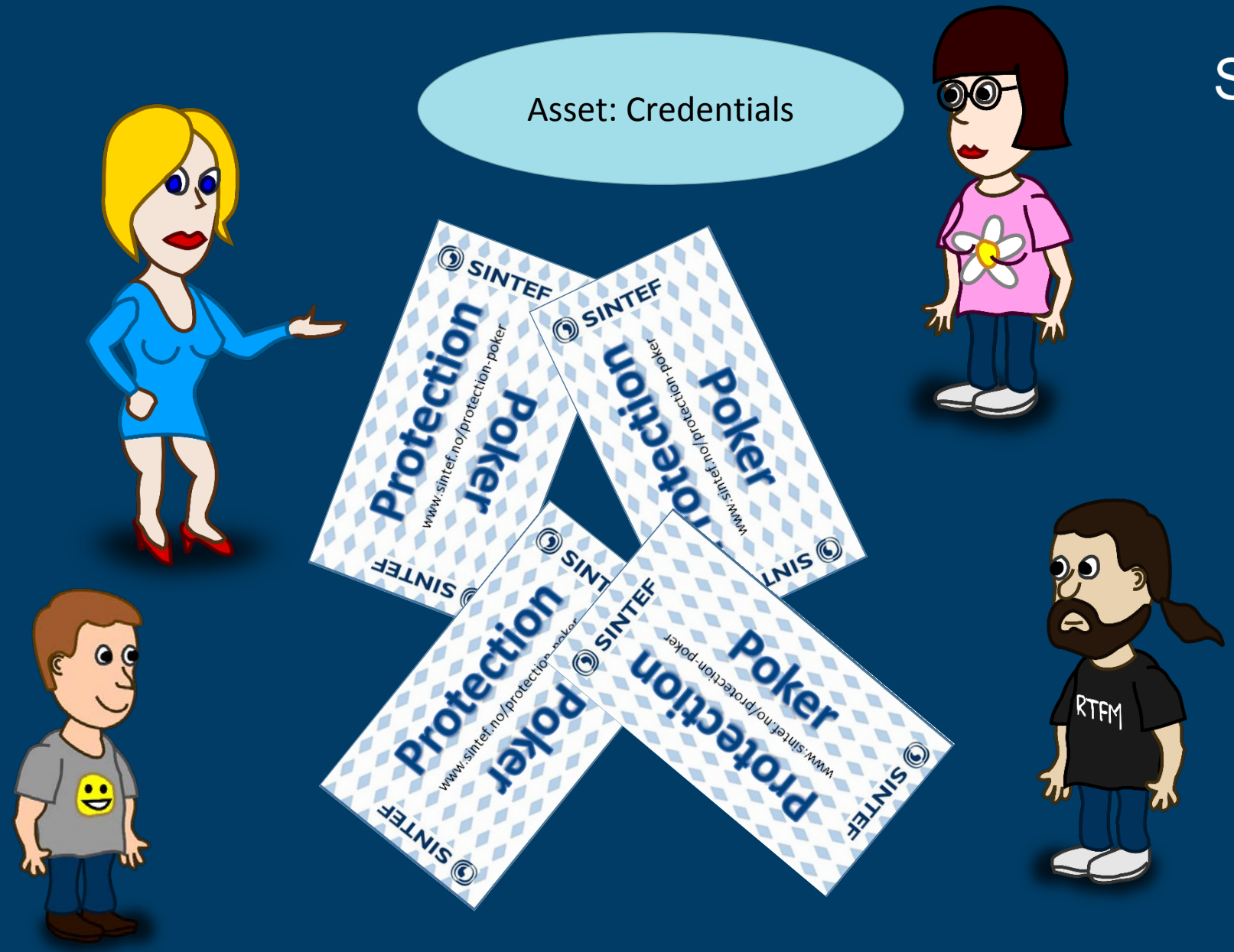
SoS-Agile

SINTEF

@seniorfrosk

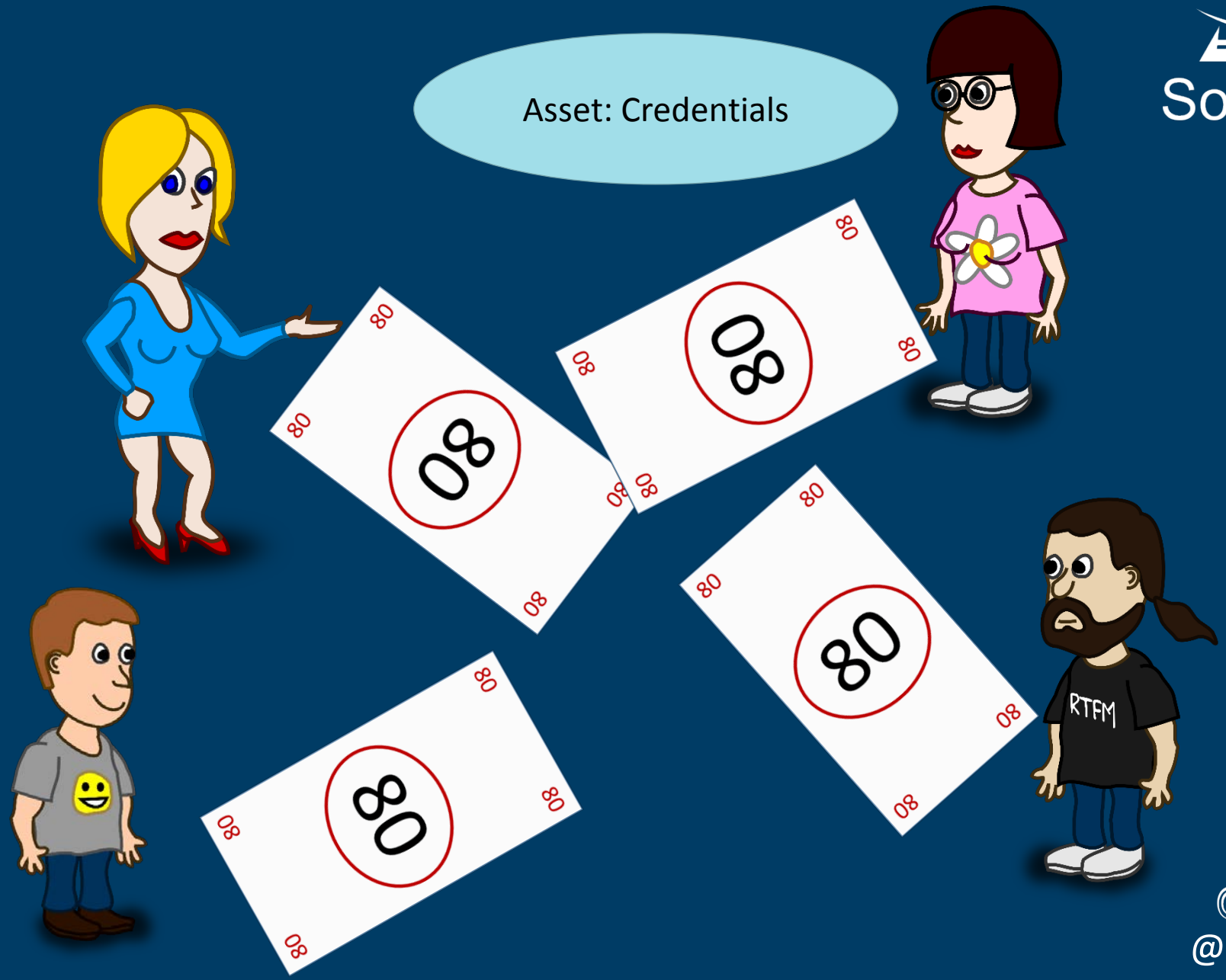
Play again! (same asset)

SoS-Agile



SINTEF
@seniorfrosk

Show your hand!



SoS-Agile

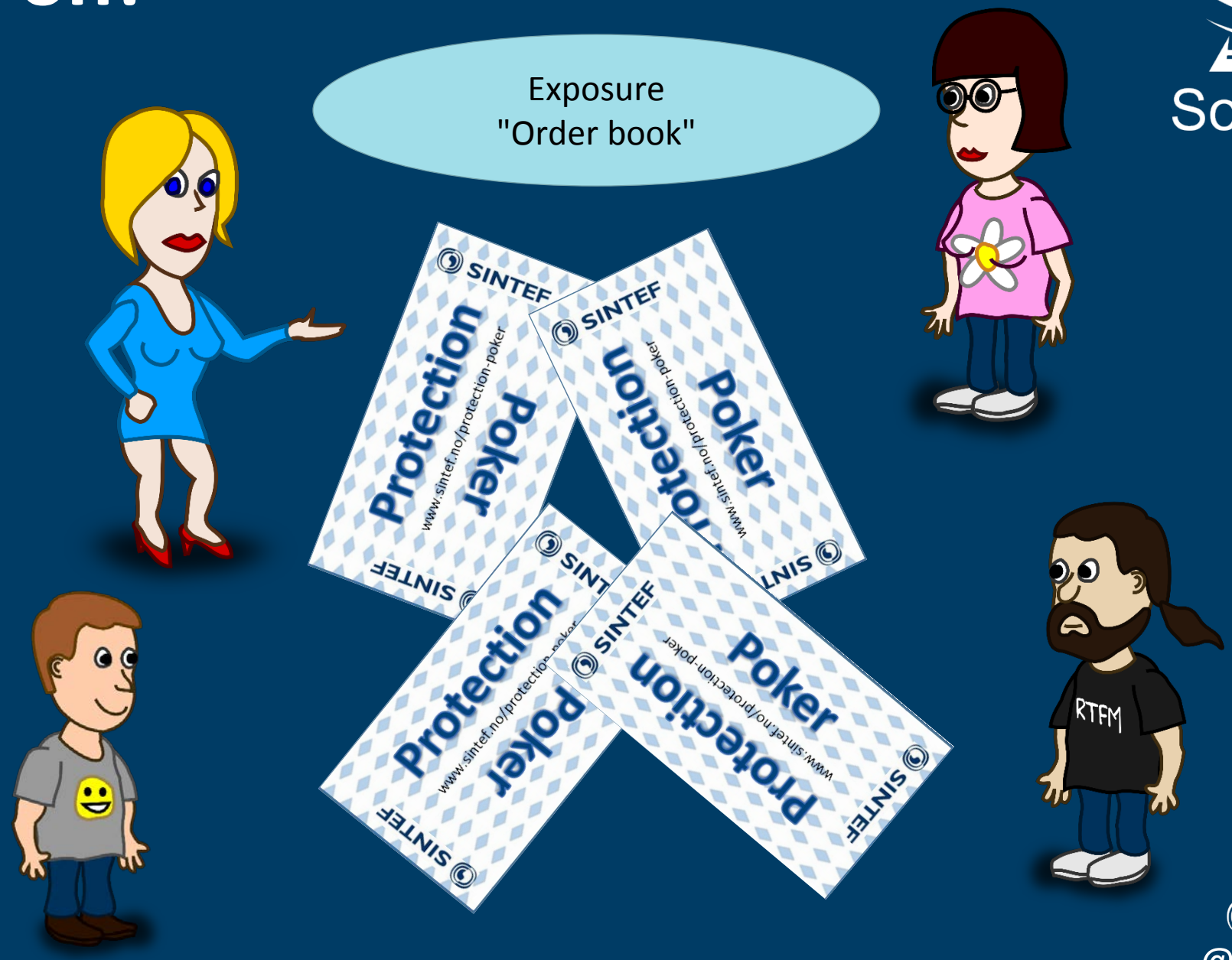
SINTEF

@seniorfrosk

(We skip the rest of the assets…)

Now: Exposure of feature "Order book"

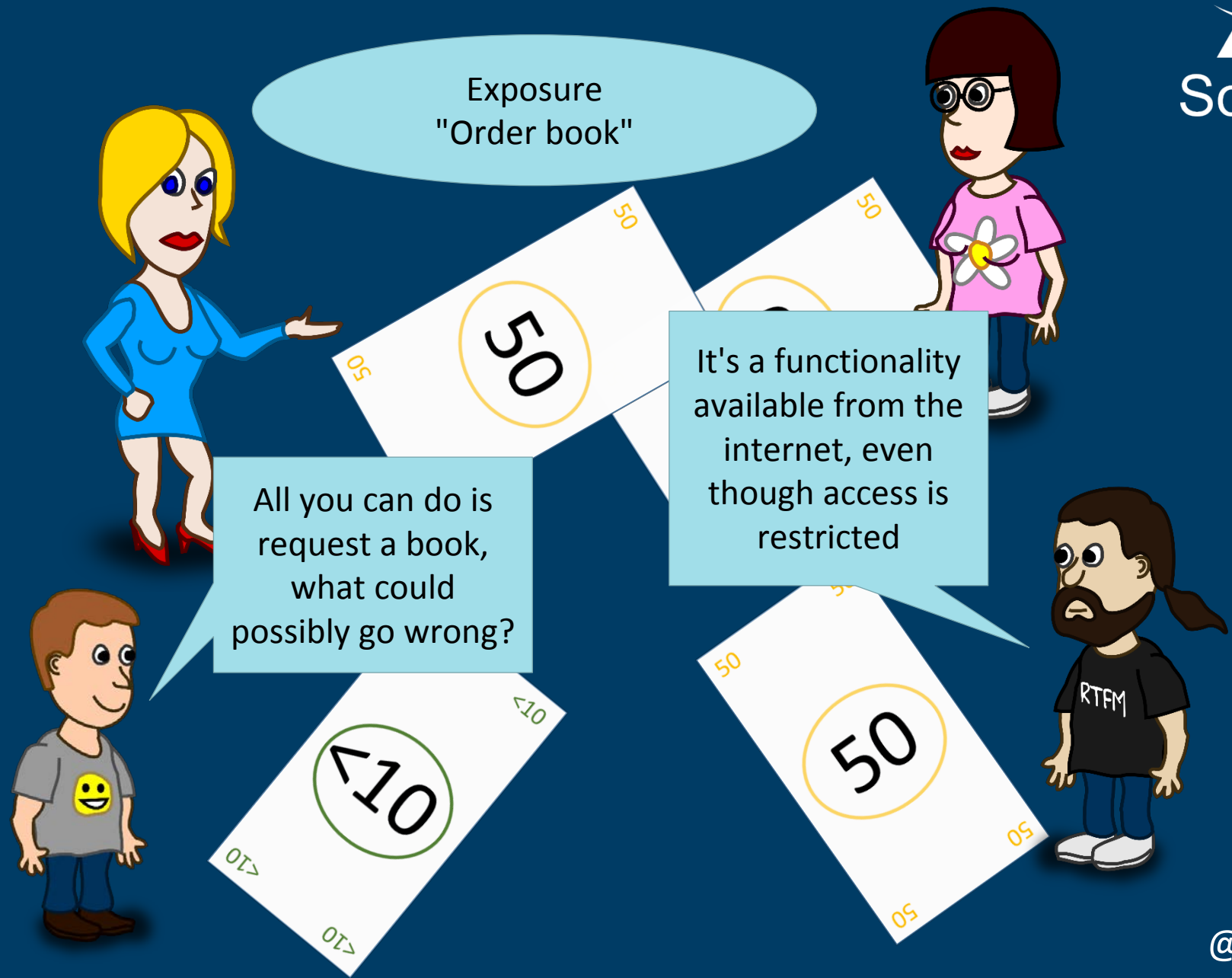
Then play on!



SoS-Agile

SINTEF
@seniorfrosk

Show cards!

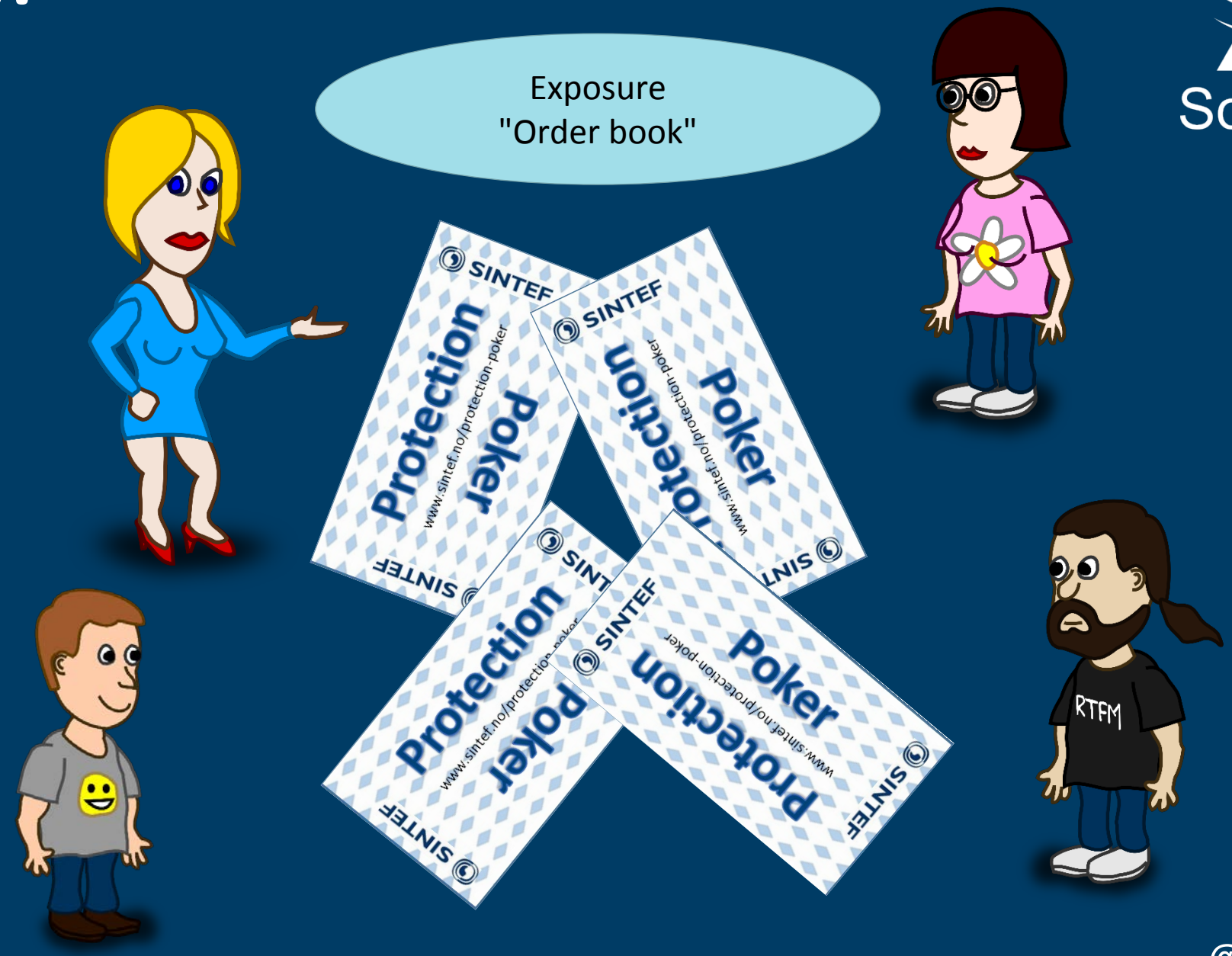


SoS-Agile

SINTEF
@seniorfrosk

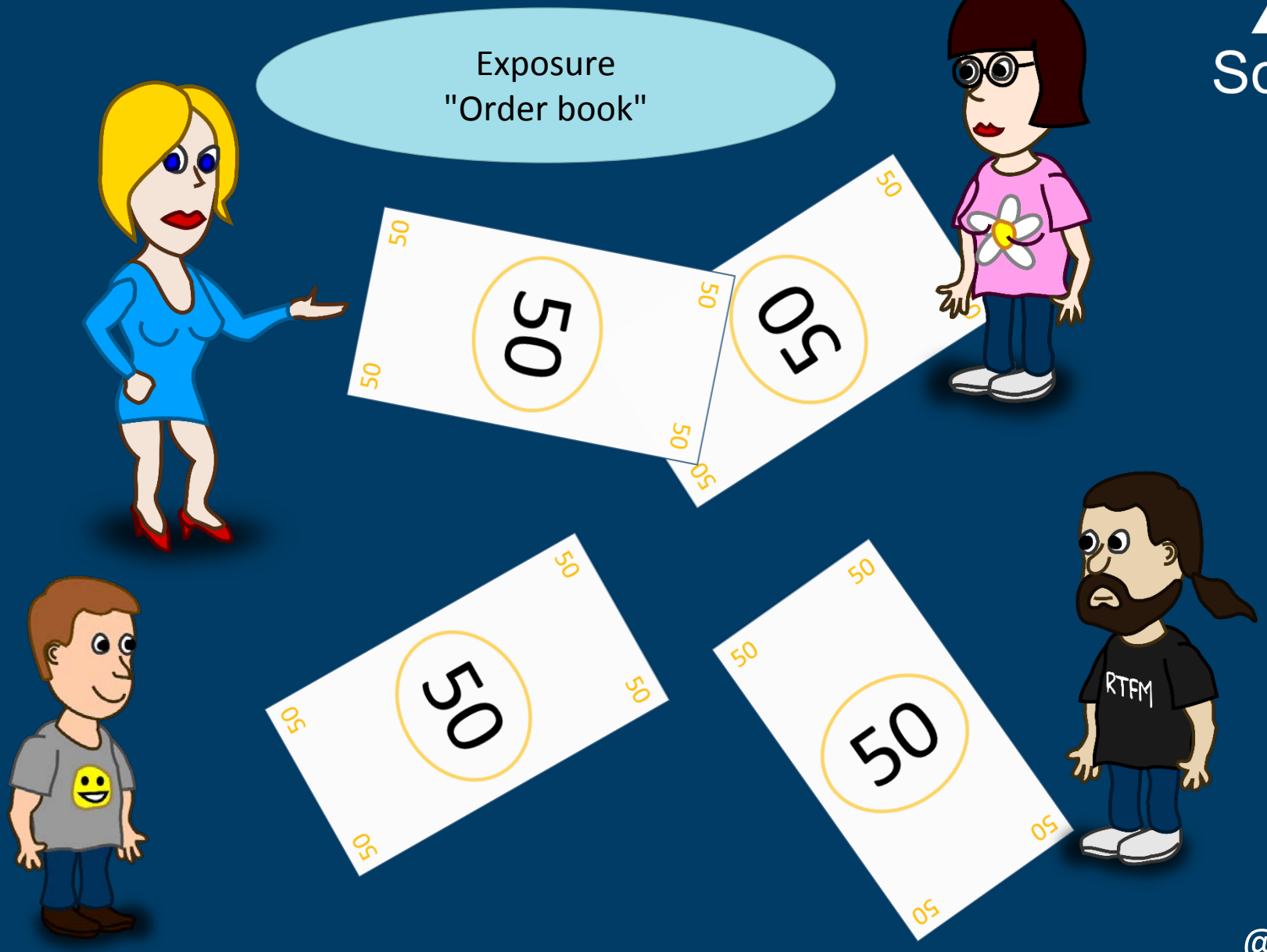
New vote!

SoS-Agile



SINTEF
@seniorfrosk

Show cards!



SoS-Agile

SINTEF
@seniorfrosk

Sum assets feature #1

SoS-Agile

#	Asset	Value
1	Authentication credentials	80
2	*Personal data*	*100*
3	*Webpages*	*50*
4	*Login session*	*80*
5	*Audit data*	*90*
6	*SQL queries*	*10*
	SUM	410

Result

#	Requirement/feature	Exposure	∑ value assets	Risk	Rank
1	Order book	50	410	20500	1
2		…			
3			…		
4	Coffe break warning	10	10	100	5
5	Add Admin user	100	150	15000	2

Calibration

SoS-Agile

- Note: The risk of a requirement is compared to that of other requirements in the same project
  - It's all relative!
- The first time one plays Protection Poker, it is recommended to do a calibration to set the end-points of the scale used.
  - Which assets have highest/lowest value?
  - Which features increase exposure the most/least?

Calibration – University Library

SoS-Agile

- Exposure

Coffee break alert

Add admin user

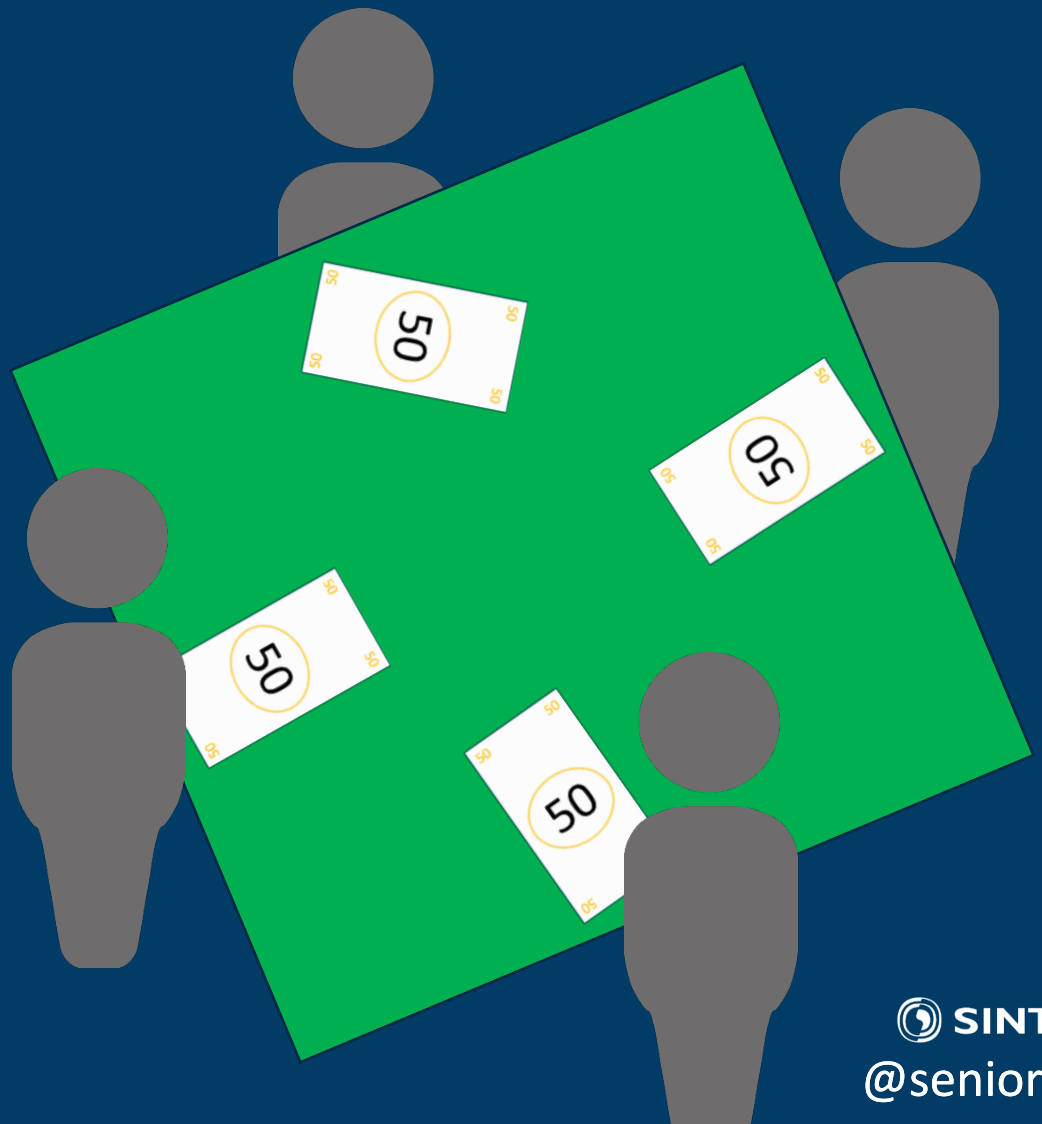
- Asset value

General library info

Personal Data

A practical tip on playing

- Keep your friends close, and your cards closer!
  - Don't throw your cards in the ring…
  - In the discussion phase, you need to remember who bid what
  - … and you need your OWN card back for the next round!



SoS-Agile

SINTEF
@seniorfrosk

Good luck!

SoS-Agile

http://www.sintef.no/protection-poker

http://www.sintef.no/sos-agile

Martin.G.Jaatun@sintef.no

SINTEF

Technology for a better society