Project plan

Name of Sandbox project: SALT

Content

Partner team members

Partner organisations: Mobai AS (Mobai), BankID BankAxept AS (BankID), Sparebank1 Østlandet (Sp1Ø), KU Leuven (KUL) and NTNU.

Partner	Name	Role	E-mail
BankID	Hanne Katrine Gulseth (HG)	Lead #1	
BankID	Michael Balner		
BankID	Dag Rinden		
Sparebank1 Østlandet	Bjørn Inge Sletta		
Sparebank1 Østlandet	Mona F. Engebretsen		
KU Leuven	Abdullah Elbi	Lead #3-4	
KU Leuven	Catherine Jasserand-Breeman		
KU Leuven	Els Kindt		
Mobai	Erik Guoqiang Li	Lead #2	
Mobai	Brage Strand		
Mobai	Petter Taugbøl (PT)	SALT PM	
Mobai	Ole Christian Olssøn	Communications	

Datatilsynet team members:

Name	Role	E-mail
Berit Bye Rinnan	Project manager	
Eirik Guldbransen	Team member	
Magnus Muehlbradt	Team member	
Hallstein Husand	Advisor	
Mirian Karlsen	Advisor	
Arild Opheim	Communications	

Short description of the project and the project plan

The SALT project ('**S**ecure privacy preserving **A**uthentication using facia**L** biometrics to pro**T**ect your identity') aims to develop an AI based authentication solution for use in both private and public sectors which will increase anti-fraud effectivity and improve end-user experience. The main motivation is to provide an advanced security-measure to prevent account take-over and identity fraud.

The increase in identity fraud and attempts is significant (10 times increases over the last two years of eID fraud) and the cost of user account takeover-related identity theft is a billion-dollar problem worldwide, a challenge that current technology does not fully solve.

The envisioned SALT solution will provide end-users with a secure authentication mechanism that minimizes the risk of identity fraud while ensuring individuals control over their personal data, as well as fulfilling transparency requirements in compliance with legal obligations.

We will present 4 issues for discussion, and we look forward to receiving guidance from the Norwegian Data Protection Authority (NDPA) in order to understand how to best research, develop and deploy the SALT solution.

The purpose of the project plan is to coordinate tasks, activities, and deliverables in the Sandbox-project. This document is internal to the Partners and NDPA, i.e., not for open distribution.

The sandbox participation objectives, project approach and expected results

The Sandbox participation objective is to explore the following issues, listed by priority:

# 1 Assess the legal status of facial images and protected templates (PT) in an AI-based solution for authentication.

Focus on legal status of facial images and PT, processing for a primary purpose of biometric authentication and for secondary purposes as fraud prevention, bias minimization and machine learning.

1. Consider processing steps from facial images to protected templates
2. Facial images and Protected templates Legal status. Issue#1 track 1

# 2 Assess the technical security measures for storing of PT to be used by the AI

The design and use of technical security measures in the SALT solution will partially depend on the results of discussions in #1.

1. Novelty of applying HM encryption

# 3 (if time allows) Assess the consequences of withdrawal of consent; do we need to retrain the algorithms?

The impact of the withdrawal of consent on existing AI and ML algorithms. The principle of lawfulness and the legal qualification of algorithmic models.

Communication plan:

A joint communication plan will be prepared. Arild from NDPA will coordinate with Ole Christian Olssøn in Mobai. Ole Christian coordinates communication activities between SALT partners.

The report will be the main results to communicate. NDPA can also bring in views from other national DPAs during the project.

The project approach:

For issues #1 and #2 we propose five workshops (2-3 hours each), both Teams and Teams/in-person, where we present and discuss the topics. In the first two workshops we will present our solution proposal for #1 and #2, respectively. In workshop three and four the purpose is to discuss the proposals, and the fifth workshop for drawing conclusions.

Results: The input will be presentations of solutions proposals (documents) and included in the final report. The output will be a paper/report (document).

Regarding #1

- Establish a shared understanding of face images, templates, protected templates and the processing activities in preforming a face authentication system
- Establishment of legal status of the facial images (including images from ID-documents)
- Establishment of legal status of images from the device live stream (realtime capture)
- Establishment of the legal status of the protected template in accordance with the respective purposes it is used for (onboarding, authentication, fraud detection, bias minimization, security improvements incl. FAR/FRR). FAR = False Acceptance Rate, FRR = False Rejection Rate).

Regarding #2

- Assessment of sufficiency of protecting the templates with homomorphic template protection encryption techniques, infrastructure construction (central/decentralized key/PT storage) and other risk treatment techniques

Secondary results: Based on the output, SALT partners may produce blog posts, contributions to research papers and other dissemination material and -activities.

If time allows**, For issues #3** we propose a workshop where we present details, our solution proposal, and to discuss and draft conclusions.

Results: Deliverables for #3 can be one report of our common understanding of the issues and possible solutions. Secondary results: Based on the deliverable, SALT partners may produce blog posts, contributions to research papers and other dissemination material.

Regarding Issue #3

- Analyzing the appropriateness of the consent as a legal basis for developing AI/ML models, including assessment of alternative legal basis
  Investigating legal status of algorithmic models used in biometric technologies (findings both from legal and technical field).

Activities, task distribution and timing

Date and time	**Topic**	**Deliverable/objective**	**Activity and method**	**Participants (responsible (in bold) and contributors)**
May 23	Kick off meeting	Presentation of SALT project, project plan and introduction to the 4 issues.	Teams meeting	**PT and HG**, All
June 7	Issue #1 Legal status of facial images and protected templates	Presentation, technical solution and data flows, preliminary legal analysis, discussion	In person meeting	**BankID** Mobai, KUL, Sp1Ø
June 29	Issue #1 Legal status of facial images and protected templates	Discussion continues, Initial version of the report to be submitted. Use case presentations Discussion continues into next meeting	Hybrid, Datatilsynets offices and Teams	**BankID,** Mobai, KUL, Sp1Ø
Aug 23	Tentative: Issue #1 Legal status of facial images and protected templates	Discussion continues, Revision of the report to be submitted	Hybrid, Datatilsynets offices and Teams	**Mobai,** NTNU**,** KUL, BankID, Sp1Ø
Sept 13	(Tentative:) Issue #2 Appropriate technical measures	Discussion continues, Revision of the report to be submitted	Hybrid, Datatilsynets offices and Teams	**KUL,** Mobai , BankID, SP1Ø
Oct 18	(Tentative:) Issue #2 Appropriate technical measures	Discussion continues, Revision of the report to be submitted	Hybrid, Datatilsynets offices and Teams	**Mobai,** KUL, BankID, NTNU, Sp1Ø
Oct -Dec	Project communcation		Articles, reports DPA's public summary	

Task list

Delivered tasks are moved from Task list to Task log.

#	*Date entered*	*TASK*	*DUE DATE*	*RESPONSIBLE*	*COMMENTS*
10	07.06	Datatilsynet: Provide first outline of final report.	27.06	Magnus	
11	07.06	SALT: Select and provide first descriptions of Use cases, with key questions raised.	27.06	Erik, Michael, Hanne, Abdullah	

Task log (finished tasks)

#	Date entered	TASK	DUE DATE	RESPONSIBLE	COMMENTS
1	*23.05*	*Distribute draft report index -*		*Hanne*	
2	*23.05*	*Share links to EAB groups and other relevant European sources of information-.*		*Abdullah*	
3	*23.05*	*Distribute the presentations from today's meeting (included in this e-mail)*	*07.06*	*Petter*	
4	*23.05*	*Confirm # of participants in WSs from SALT partners: Petter*	*07.06*	*Petter*	
5	*23.05*	*Send out meeting details for the June 7 WS ..*	*07.06*	*Berit*	
6	*23.05*	*Share a draft index of the final report,*	*07.06*	*Eirik*	
7	*23.05*	*Establish a "project space" where we can share documents / work on the same documents-*	*07.06*	*Petter*	
8	*23.05*	*Prepare Flow diagram of solution, from facial images to protected templates, especially highlighting personal data. Both untrusted and trusted client device.*	*07.06*	*Erik*	
9	*23.05*	*Prepare input for discussion on issue #1, track 1.*	*07.06*	*Michael, Hanne and Abdullah*	