Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark – Usefulness, Barriers, and Recommendations

MADS SCHAARP ANDESEN, The Alexandra Institute A/S, Denmark

In this paper, we explore why partial identity technologies such as privacy-preserving attribute based credentials (pABCs) have been around for a while without getting adopted in real life identity solutions and how we might design for such technologies. This is done by exploring whether this is perceived useful from the user as well as the service provider side through the design of a digital identity solution in Denmark. Two interview studies with three and 11 participants representing service providers and users, respectively, were carried out and a design for a digital identity solution was created. The results show that while there is a use for such technologies, there are certain issues that need to be considered. Based on the results, we present 8 design recommendations on implementing a digital identity solution based on pABCs. For future work, we suggest that these studies should be repeated in other national contexts to explore how general the results are.

ACM Reference Format:

1 INTRODUCTION

Partial identity technologies have emerged as a valuable way of providing users with the ability to reveal only specific attributes of their identities or assertions upon these while, through cryptographic techniques, still providing proof that the revealed is true and based on the full identity. Another feature of these technologies is that when the (partial) identity is used, the identity issuer (often called IdP or Identity Provider) cannot see where the identity has been used – a feature called unlinkability – thus ensuring even more privacy for the users. This has a lot of potential in a post-GDPR world in which data minimization is a requirement. However, even though technologies like these have been around for a while, e.g., Privacy-preserving Attribute Based Credentials (pABCs) as developed in the ABC4Trust project [11] and implemented in Identity Mixer [6] and Microsoft UProve [7], they have yet to be used in a larger scale deployment. This begs to ask the question of why that might be.

In this paper, we explore this question by examining whether there is a pull for this technology and whether that might come from service providers that need to verify users or the users themselves. We do this using a user-centric approach in order to explore how we can design a user experience for an identity solution based on pABCs in Denmark. The studies done are part of the EU Horizon 2020 OLYMPUS project [9].

The first part of the work was a pre-study in the context of the Danish commerce sector to explore whether a pull from service providers exist. We conducted a small three-interview pilot study with representatives of Danish supermarkets. Here we found that there is currently some pull for technology that can make it easier for the stores to verify age of shoppers.
To examine whether there is a potential for pABC-based technologies amongst users, we designed a pABC user experience for an app and conducted a series of qualitative interviews in which the design was evaluated and, furthermore, attitudes and knowledge on different aspects of security, privacy, and identities – physical and digital – were explored. We find that the proposed design with minor changes would be a useful design and concept for users. Furthermore, we find that users have differing views on digital vs. physical-ids and that it is important to consider the differences of these in the design. Another important find is that trust is one of the most important factors in deploying a pABC-based identity solution and, that in the Danish context, users trust public authorities over private companies with regards to handling identity. We also find that users in the study do have some concerns in regards to security on the Internet, sharing personal information, and using physical ids, but that this does not prevent people from sharing personal information online or using their physical id to verify identity.

Finally, we propose a number of design recommendations for pABC-based technologies including a set of eight concrete design guidelines.

2 RELATED WORK

Not much work exists about the human factor aspects of pABCs. Wästlund et al. [16] and Wästlund and Fischer-Hübner [15] investigate the challenges of conveying the privacy properties of pABCs to the users. They find that users have a hard time creating the correct mental models due to lack of real world analogies. Benenson et al. [2, 3], did an explorative study of course evaluation based on pABC technology. This was done to assess the user acceptance level of pABC-based technologies. They find that the technology is perceived useful for protecting privacy and that understanding of the technology was correlated to perceived usefulness. Hence, understanding the technology is seen as a major barrier to adoption.

In the study most similar to ours, Sabouri [13] conducts a study of a mock pABC-based id card. In the study the users have to use the technology for discussing politics online. They find that users were about to see the privacy protection benefits of the technology. Trust is also identified as one of the main barriers of adopting the proposed solution.

Compared to the work presented above, our work focuses on introducing a pABC-based digital ID in a situation in a familiar everyday situation in which users are used to showing some form of ID, typically a physical one. This enables us to study how participants perceive the usefulness of pABCs in relation to the ID they are currently using in the same situation, thus enabling us to explore how pABCs might be introduced as an alternative to existing IDs.

In relation to the adoption of pABCs by service providers, Sabouri [12] create a conceptual model of the relevant factors for adoption of pABC technology and evaluate this with experts in the field as the technology is not yet available. In our work we take a different approach and explore how pABCs might be adopted by service providers by talking directly to the service providers.

3 PILOT-STUDY: DO COMPANIES NEED PABC TECHNOLOGY?

We carried out three qualitative unstructured interviews with the purpose of getting an understanding of whether the pull for pABC technologies might come from companies. Two interviews were carried out with two large organizations representing chains of Danish supermarkets and convenience stores, and one interview was carried out with a manager of a large Danish supermarket.
3.1 Results

The two organizations mentioned that they were currently working on a solution to include information on whether or not a person is above the age of 18 in the Danish debit card solution: Dankort. The idea was that when a user makes a payment with a Dankort, the system will automatically tell the shop assistants whether a person was allowed to buy, e.g., alcohol or not. Hence, there seems to be some need for a better way of checking the age of customers than looking at an id-card. This was further supported by the manager who expressed that his shop assistants sometimes had a hard time decoding the age from a birthday on an id-card. This process can sometimes take time and can lead to embarrassment for the shop assistant which might lead to a less thorough verification of the id-card. This had the negative effect that, besides potentially causing a person below the legal age to buy alcohol and/or cigarettes, rumor spread quickly and suddenly a lot of underage people might show up to buy items they were not allowed to. This was a real fear for the manager, as it could lead to a larger risk of fines and a lot of bad publicity. Every year, the Danish newspapers send out young people below the legal age to see where they are able to buy things they should not be able to (e.g., [10]). Furthermore, the manager explained that the systems in the store today prompt shop assistants to verify that they have seen proof that the shopper is above the legal age. This puts a lot of responsibility on the shopping assistant in a pressured situation, which an automated technology might help alleviate.

The above indicates that there is need for some way of helping shop assistants make faster and more accurate decisions. While the idea to embed the age check in the debit card seeks to help this problem, it does, however, leave it open to borrowing someone else’s card, hereby skipping the check of whether the person using the card is the owner. Hence, it seems that a solution which includes pictures would be useful.

The pre-study shows that there is a need and pull for a better solution in supermarkets which can somehow help the shop assistants determine whether a person is allowed to make a purchase or not.

4 DESIGNING A PABC EXPERIENCE

Based on the pre-study, internal brainstorming, and informal talks with OLYMPUS-project partners, a pABC user experience was designed. This was based on the idea of being able to use pABCs as a general identification method from which identity proofs could be created of the form: This person is at least 18 years old, This person is a Danish Citizen, This person holds a valid drivers license, etc.

For users to understand how pABC-based technology can be used, we designed an elaborate user experience and concept. This is based on a scenario with the main character Jens, who is asked to buy a bottle of gin for his parents. He is 18 years old – the legally required age to buy alcohol in Denmark – but he looks younger, so he is always asked to show his ID when making purchase in which one has to be 18. The scenario shows how a potential smartphone pABC app can be used in a real world situation in which many of us can relate to and/or have experience at some point. Either by our own experience or through friends and relatives, or even as a bystander.

During the design phase, emphasis was put on constructing a scenario with sufficient granularity so people could recognize the situation and could identify themselves to some extent within the situation. As such, the visualization can also be considered to be a probe or at prototype, used for collecting people’s response on specific issues.

5 INTERVIEW STUDY: HOW SHOULD WE DESIGN PABC-BASED IDS?

This section documents the interview study that was done to evaluate the design presented in the previous section and gain insights into participants’ view on security and privacy as well as their use of IDs.
The study was motivated by trying to determine whether there is a perceived need for pABC-based technology and how such a solution should be designed and deployed so that it creates the biggest value to citizens.

5.1 Participants

11 interviews were conducted with Danish consumers. These were recruited using an external recruiting bureau. This was done to get a broad representation of Danish consumers as the bureau has an established consumer panel and, hence, would be able to get a good representation. Participants were recruited to have a broad representation of: educational level, age, and gender. Participants should be at least 18 years in order to have experience with identifying themselves with the situation of buying alcohol presented in the design of section 4.

Demographics. Participants’ age range from 20-67 and have an average age of 42.8 with median 45. There were 6 women and 5 males. In terms of highest finished education, they had: 9th grade (1), high school (1), lower degree (1), bachelor or similar (3), master or similar (5). All were working or under education.

5.2 Method

The interviews were carried out as qualitative, semi-structured interviews lasting approx. 45 minutes each. The interviews were carried out using Microsoft Teams and interviews were recorded and transcribed, anonymizing the participants in the process. Consent forms were sent to participants as part of recruitment and oral consents were obtained in the beginning of the interviews. The transcriptions were qualitatively coded and analyzed. During the interviews the design from the previous phase was presented by the images found in Appendix A. The interview guide had the following topics:

- **Demographics** Questions about the participants. How they are, what they do.
- **Online Security and Information Sharing** Questions about how secure participants feel on the Internet and what information they share and how they feel about that. In particular questions relating to the sharing of CPR-number (Danish Social Security Number) and use of NemID [8] (Danish national digital identity solution).
- **Physical ID-cards** Questions about where and how often they use physical ID-cards, how secure they feel using them and how they perceive threats in doing so.
- **Misuse and Identity Theft** Do they feel at risk using their identity (ID-cards or digital)
- **pABC Identity Solution** After getting a presentation of the pABC design developed, participants were asked about their thoughts on the solution, whether they would use such a solution, and other thoughts surrounding the presented design and the pABC-based technology.

Two researchers – a computer scientist and a designer – conducted the interviews. Both researchers analyzed the interview transcripts.

5.3 Results

In this section we will present the main results from the interviews. All interviews were carried out in Danish, and the quotes from the participants have been translated into English.

5.3.1 Trust is a Main Factor in Feeling Secure. During the interviews, some of the participants had some basic misunderstanding of how the technology worked regarding the amount of information shared and the unlinkability guarantee. In order for those participants to understand what was going on in the scenario, further information was provided. This
was done to make them understand that when using the system, no other information was shared that the verifier actually sees. Two participants mentioned that they thought that the store using the pABC system would be able to backtrack the information shared by the user to extract the original data, and two expressed a concern that their data would be logged. One of them mentioned a fear that it would be used to keep a trace of whenever he/she had bought alcohol. After the interviewer explained that this was not the case, the participants expressed that they now understood the system and that it felt secure. When asked about what it would take for them to understand that the system was secure, one mentioned that this should be communicated in some form before he/she would even consider installing the app. Another mentioned that this should be explained in a consent form, while at the same time revealing that he/she almost never read these. Several participants expressed that as long as someone had vouched for the solution, they felt secure. Hence, it seems that trust in the organization providing the app or an organization vouching for the app is more important than explicitly explaining the guarantees as part of the app. This is explained by P7: “So no, I don’t think there is anything [bad] in the concept you have presented – apart from the trust.” highlighting that trust was the main factor in choosing whether or not to use the app.

When asked who should provide a pABC-based app?, all participants replied that it should either be provided by some public authority or at least be approved by a public authority. Most participants mentioned the state or some authority under the state as either providing the solution or vouching for the solution. P8 expressed that: “[The state] has to test it many times and will be held accountable if there are errors in [the system] vs. private companies. It’s a different reality”, highlighting that he/she believed that the accountability of the state would not apply for a private company. Two participants mentioned that NemID (or NETS, the company behind the NemID solution) would induce trust as they already used and trusted that. While it might seem strange that all the participants had such a high degree of trust in the Danish state, this is supported by research that Scandinavia has the highest degree of trust in the world [1, 14].

5.3.2 Physical IDs are Often Considered to Be Safe Enough. The participants used a variety of different physical-ids: health card, drivers license, travel card, passport, student id, Dankort (Danish debit card), and a variety of membership cards. They expressed using them in the following situations: picking up packages, traveling, buying alcohol, getting into bars, going to the doctor. The main reason for having to identify themselves was picking up packages, either at the post office or at other couriers. Some participants expressed that the need to pick up packages had increased a lot during COVID-19, and most participants expressed the need to identify themselves when picking up packages.

When asked about whether they had thought about what information they were actually giving up when identifying themselves with a drivers license when picking up packages, half of them expressed that they had not given it much thought and one even stated that he/she did not think that the information on the license could be misused. P2: “[There is] no information [on it] that would be able to be misused for anything.” A fourth of participants did not think that a CPR-number – something most expressed being of particular importance to safe-keep – was even on a Danish license, which it is! Most other participants did, however, know that the CPR-number is printed on the license. Some participants expressed that they thought of the information on the Danish health card as being more sensitive than the information on the drivers license. The two young female participants expressed particular worry about someone getting a hold of their health card information, which contains their name and address – and is very visible – as they were worried that someone might try to contact them – something no other participants addressed.

The participants were also asked whether they or someone they knew had had their information misused in any way. When answering this question, two thirds expressed that they or someone they knew had experienced some form

---

1 A Danish health card has address and doctor which is not present on a license.
of misuse. However, for all but one participant this was related to payment cards and monetary loses from that (which in Denmark is usually covered by the bank). The one person who knew people having their identity misused knew of a woman having her information shared on a dating website and he/she had two friends who had their NemIDs misused to take out loan in their name. Several participants also mentioned that they were more worried about having their debit card details stolen than their identity information. Finally, a third of the participants mentioned that they found that the verification was so swift that the verifiers would not be able to really see the information on the card, hence, making it secure. Most participants were not really worried about showing their ID. Two questioned whether the case of buying alcohol presented to them, was really a situation where people got swindled. As P5 put it: "...is the shop assistant in COOP our primary suspect?". Overall, there was a feeling among most of the participants that showing their ID is not a threat. P6 expressed: "The nice old ladies in Kvickly do not occur to me as being a security risk" and P8 said: "[Bouncers] have never struck me as being the type who will go home and hack me".

5.3.3 Keep Everything in One Place is Both Good and Bad. During the interviews an interesting duality occurred. Many participants really liked the idea of eliminating the need to carry around physical cards and having everything in the same app. At the same time participants – often the same who expressed the advantage of keeping things in one place – also expressed some security concerns with having everything in one app. What if their phone was stolen? However, several participants reflected over the fact that the same could happen if they would lose their wallet. Some even expressed that a smartphone in that regard, has the advantage that there are additional security mechanisms in place, which do not exist in the physical card world. As P9 put it: "You can lose your wallet and then you lose everything [...] Many people have their phone stolen, but it is not easy to gain access to it. [...] There are all sort of passwords, face-id and fingerprints."

In relation to having identity information on the phone instead of a physical card, two participants mentioned it as a problem that a phone can run out of battery.

5.3.4 Digitalization is Coming... But we are Not All There Yet. When asked the hypothetical question of whether the participants could see themselves use the solution presented, most said yes. As P11 puts it: "Yes I would [use the app]. Are you crazy?! Then you have it on your phone. Then you don’t have to get out your card". P9 also expressed a desire not to bring any cards: "...without having to bring everything. For example during the summer. Then I don’t wear a giant jacket where I can have stuff in the pocket." However, two participants did express that they would rather show their physical ID because they find it to be faster.

Throughout the interviews, there was a tendency that the younger people are, the less they are carrying a physical wallet. Furthermore, they were more willing to use a smartphone-based identity solution. As P10 puts it: "Maybe it is more for the young generation? [...] I don’t have a payment or bank app on my phone [...] my son doesn’t feel [the same way]. He would use it more and thinks that it is easier to use an app."

5.3.5 A Need to Consider Edge-cases. As expressed earlier, the two young women were afraid that their addresses might be used to contact them. As P3 expressed it: "...I have thought that the person who is checking could contact you, even though it is in a professional situation [that they are checking id]... that they remember you because of something" and P11 said: "...there just has to be one standing behind you, then he has everything." Furthermore, P5 mentioned a case in which Danish celebrities had their purchase histories shared [17] and P1 said: "It doesn’t matter for someone like me, but what if you were a celebrity? Then you might not be as willing to share your address". This shows that even though not

---

2A Danish chain of supermarkets.
everyone finds it relevant to hide details of their information when identifying themselves towards the shop assistant at a package shop or towards a bouncer at a bar, some people do indeed have this need, and we should remember to design for these groups. In the interviews, this seems to be especially true for the young women. Several participants also mentioned that we should not forget the old generation. P11 said: "...we might lose the elder population on [digital solutions]. They have a tendency to give up before they try it., so it is important to consider how they might use a solution like this, and if they do not, provide an alternative.

pABC App Design
The following describes the results from the interviews directly related to the app concept presented.

5.3.6 Time is a Factor. Several participants expressed that it was important that it is fast to use. P6 said: "If you have to find [in the app] Salling Group, SuperBrugsen, and another GLS pickup3 spot. Then it loses its 'smart' if it is not super fast." Two participants also expressed that they might use physical ID if it felt faster.

5.3.7 Design is Somewhat Laborious. Several participants expressed that the design was too laborious with too many steps. P4 expressed that it was tedious to have to do it for every store: "I think that would be my suggestion. Eliminate some step so you can go from store to store. I would get annoyed [if you could not]." This view was shared by a forth of participants. However, the same participants also expressed that they would use the solution with minor changes to the design. Some participants also expressed that they would prefer that the app would show the minimum information needed rather than that they would have to choose it themselves as it might lead to over sharing. As P1 put it: "I have an old mom [...] who doesn’t really think that much about what she has crossed off".

5.3.8 Wide Adoption Would Be Needed. Some participants also expressed that in order for the pABC app to be desirable, it would need to be usable many place. P5 goes as far as saying: "The ideal would be that this was our general identity on the net."

5.3.9 Good Idea to Limit Information Sharing. Half of the participants expressed that the idea of being able to limit how much information was shared was a good idea and something they would use to some degree. P7 said: "I like the idea that I can choose what information is passed on. The thing that the person, the shop assistant here, only gets exactly the information which is needed and nothing else."

5.3.10 Security Guarantees Can Be Hard to Understand. Just under half the participants found it difficult to understand exactly what the security guarantees of the underlying system were. Two participants believed that the store would store a lot of information. As P5 put it: "Your system would store a lot(!) of information in the background. We could, until the day the server is deleted, be able to track that Jens4 at the age of 18 years and two minutes went down and bought a bottle of Gin." and P8 expressed a concern that the store would be able to see the full identity: "They can probably see how old you really are." There was also some confusion as to whether QR codes would actually contain the entire identity.

6 DESIGN GUIDELINES
Based on the results, we propose the following set of eight concrete guidelines of how to design a user experience around pABC technology.

3 All three are examples of stores and package couriers in Denmark.
4 Jens was the person described in the scenario presented.
6.1 Eight Design Principles for User Experience and pABC-based Technology

The following acts as a set of guidelines for how pABC-based identity solutions should be designed for deployment in a Danish context.

1) A Public Authority Should Run or Vouch for the Solution. With the high degree of trust in public authorities, it is important for wide adoption of a general pABC based identity solution that it is either offered by a public authority or approved by one. Basing the system on already known IDs can be beneficial for trust. In Denmark, this could be the drivers license, which has recently been digitized, or NemID – the national digital identity.

2) Explanations of Security Guarantees Should not be Present in the Primary Layer. Since our research showed that trust in the provider rather than explanations of how the security of pABC technology works, we propose that explanation of this technology should be kept in the secondary layer, so that users interested can read about it, but keeping it out of the way or ordinary users who place their trust in that the provider does not store traces of activity or will be able to recreate identities from identity proofs.

3) Solution Should Be and Feel Fast to Use. For people to use the solution it is important that it does not seem like a hassle to use, as this might make people use their physical ID instead. The solution should therefore have as few steps as possible to create and use the identity proofs. The identity proof should, furthermore, be agnostic as to where they can be used. A standard of what is needed to, e.g., pick up a package or buy alcohol should exist.

4) We Should Design for Edge Cases. Even though most people might not see the need to hide specific information, such as address, others might have a need or wish to hide their information. This could be celebrities, people who have problems with stalkers, or have some other reason for wanting to limit the information they share about themselves.

5) The Identity Should be Widely Usable. It is important for the adoption of an identity solution based on pABC-technology, that it is possible to use it in so many places as possible. If only some stores support it, users shopping between stores will have to carry their physical ID anyway, making them less likely to install the app. If possible, the solution should also be available across borders so that a person working in Copenhagen, but living across the bridge in Sweden, can use his/her ID in both countries.

6) The Solution Should Support Many Types of IDs. As a Danish citizen, there is a need to have different types of IDs: The national health card, the European health card, drivers license, passport, membership cards. If an pABC identity app could handle all these types of IDs, it would be more likely that it would be used.

7) The Solution Should Also Focus on Helping the Verifiers. In situations, such as the shop assistant verifying age, it is also important to design for the shop assistant as to help them make the assessment of, e.g., age easier. They do not want to see the unnecessary information present on physical IDs and they do not want to calculate age based on a birth date.

8) Public Information of How the Technology Works Should Be Prioritized. As users place their trust in the provider of the technology and that they would decide whether or not to install the app before, it is important to create public information campaigns to explain exactly what the technology can offer and how it differs from existing solutions such as using Facebook login where a lot of information is traced by Facebook. The solution needs to distinguish itself from the surveillance capitalism-based solutions.


7 DISCUSSION

As documented in this paper, our research has shown that there is potential for an identity app based on pABC technology. Furthermore, we have also seen that there is a use for an electronic identity which could be used instead of the physical cards and this seems to be truer the younger and more digital natives the users are. In Denmark, some of this functionality is already available in form of the digital drivers license [4]. However, this is limited to two views on the information and does not provide the ability to be electronically verified in supermarket, i.e., it would not solve the issue of helping the shop assistants. There does seem to be a use for the more elaborate solution that the design of the pABC app in this paper does.

From our results, it seems that age plays an important role in how willing people are to move from physical ID-cards to a purely digital version. This is not surprising as younger people are digital natives, i.e., they have grown up with smartphones and the Internet. We see this is that they only carry their physical IDs when they really need to, and would prefer just to carry their phone, and hence, seem more willing to accept that it might take a little more effort than pulling a card from your pocket. For the people who prefer the swiftness of using a card, it is an important requirement for a digital ID solution that it does not feel significantly slower than using the physical card.

The results also indicate that at some point in the future, it will be possible to replace the physical card entirely, but until them, it is important to remember to design for the people who prefer physical cards. Furthermore, it is important that we cater for the elder generation who have had digital technology introduced rather late in life.

In relation to trusting whether a solution is secure and does what it claims, we found that trust was a very important factor in deciding whether or not to believe something is secure. In fact, none of the participants asked for a detailed explanation of how the technology works. This indicates that they trust an organization vouching for the system more than they trust their own ability to understand complex security. Hence, we believe that emphasis should be put on explaining who the provider of the system is, rather than spending a lot of effort explaining security to regular users. An explanation of complex security models is, however, still relevant so that experts can make judgments on whether something is indeed secure or not. The effort should be spent on explaining to experts not regular users. This is also interesting as it is in opposition to the results by Benenson et al. [3] in which it was found that the more the participants understood the technology, the more willing they were to adopt the technology.

In terms of trust, it is also interesting that our work showed that in general, most participants found that in the situations in which they had to show their ID cards, they were not worried about their information being misused. This indicates that there is an inherent trustfulness towards fellow citizens in Denmark. This is also supported by the work of Svendsen [14]. This indicates that the results might not be generalizable to other contexts, and that similar studies as the one we have conducted, should be repeated in the context in which the solution should be deployed. That human subject studies are not always generally applicable is also supported by the theory of WEIRD people by Henrich et al. [5]. Hence, it would, for all purposes, be interesting to conduct similar studies to explore how general the results of this paper are.

8 CONCLUSION

In this paper, we explored whether there is a pull for an pABC-based identity app for Danish citizens and for stores with a need to verify identities. We find that, in large, the participants in our user studies think that such a solution would be useful in gathering everything in one place, eliminating the need to carry a lot of physical cards around, and being able to minimize the information shared. We also developed an elaborate design of how such a system might
work in order to get the specific feedback needed to develop our design guidelines. Furthermore, we found that such a solution should be hosted by a trusted party, which in Denmark means a public authority or at least a solution should approved by one. We find that overall, trust plays a large role in deploying an advanced identity solution. Even when participants had problems understanding exactly how the security guarantees of pABCs, they trusted that if the state was somehow involved in the system, it would be OK. Hence, we found no wish from the participants to explain the technology in detail in the app, but rather found that it was needed as part of a communication strategy surrounding the release of such an app. Finally, we created a set of eight design guidelines and which should be used when deploying an pABC-based app in the context of Denmark.

9 ACKNOWLEDGEMENTS

This work described in this paper has been carried out as part of the ObLivious identitY Management for Private and User-friendly Services (OLYMPUS) project which has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786725 (OLYMPUS).

REFERENCES


A THE OLYMPUS APP DESIGN

In Figure 1, 2, 3, 4, 5, and 6 the steps of the design and user experience are show as presented in the interviews.
Fig. 1. Jens has been asked by his parents to buy a bottle of gin at the supermarket. He is tired of having to show his ID just because he looks younger than he is, so he downloads the pBAC app. He opens it and verifies with NemID and chooses the store (COOP) that he wants to use it in and what he wants to use it for. In this case, he wants to buy alcohol and therefore he also chooses that all he wants to show is his age and a photo. The app then tells him that the app can now be used in COOP.
Fig. 2. Jens arrives at the supermarket, finds and grabs the bottle of gin and goes to the register shop assistant. As expected, she asks him if he has ID.
Fig. 3. Jens takes out his smartphone in order to be able to show ID, and the shop assistant gets ready to verify his ID.
Fig. 4. Jens opens the pBAC app. He chooses COOP – the shop he is in – and chooses verify age. The app then shows his photo and a QR code.
Fig. 5. Jens shows the screen with his photo and the QR code to the shop assistant. She takes her COOP smartphone and scans the QR code. Her phone then shows Jens’s photo in combination with a message that the customer is over 18 years old.
Fig. 6. Jens leaves the supermarket with a bottle of gin.