Interviewer: You can introduce yourself and talk about your experience first, and afterward I will ask some navigational questions if that's easier.

Expert: Sure. I started on the cusp doing reverse engineering of the NemID app for my bachelor's thesis. My co-student and I learned quite a bit about how it works and ended up submitting a couple of things we thought they could do better, including one thing we really thought they should fix.

After that, I took an interest in citizens' digital identity as we were moving from NemID to MitID. There was a lot changing during this transition. I became interested in keeping track of it because they were redesigning the whole system, and there were bound to be problems associated with that. It's been interesting to find issues and challenge myself to understand how it works, especially since they don't really want people to know how the system works for some reason.

This has resulted in me submitting 4-5 different bugs I thought should be fixed. Maybe 2-3 have been directly fixed after I reported them, while some issues weren't addressed immediately but were fixed later.

As “Person X” may have told you, it all culminated with me completely reverse engineering MitID, which resulted in them making it harder to create a custom app by relying on Google and Apple for validation. They claimed they were already planning this change, but you never know if that's true. This approach really locks down the app, preventing people from running it on alternative operating systems.

I've had experience talking with Digitaliseringsstyrelsen and the private companies they contract with. I've identified pitfalls in how they handle these social situations. MitID and NemID are critical pieces of infrastructure, and security should always be the top priority when handling issues from people like me. I've done my best to maintain good terms with them, but they still don't trust me and treat me as if I'm a threat rather than a help.

One of my biggest complaints is that it feels very political when you report something. If it's a small security bug they can fix right away, they're happy about it. But if it's not small—if it's structural—you can feel political pressure. They won't admit there's a problem or they'll shut you down with no real idea of when the issue will be fixed.

The biggest issue I encountered was when we discovered you could find people's usernames in MitID by simply enumerating them. Previously with NemID, there was a classic username and password system where you had to enter both, then use your card to type in a code. Later they added an app you could swipe, but you still needed a username and code.

When MitID came out, it only required a username with no password involved. This concerned me because it ruined many of the guarantees from a username/password system. On the first day of launch, I typed in a common Danish name like "Henrik" and the system recognized it, indicating you could easily guess people's usernames.

Because of a different change they made—possibly related to something we had reported—if you type someone's name into the field, they cannot log in elsewhere at the same time. This was to prevent timing attacks where users think they're logging into their own account but are actually accessing yours. If you knew someone's username, you could block them from using MitID. This was so easy that you could potentially block thousands of people from logging in.

This was a structural problem with the design. The security algorithms they use are actually quite good, but someone must have decided it would be easier, especially for older people, if it was just a username. It is simpler, but it's also very problematic from a security perspective.

Because they didn't want to change this decision after it was announced as a feature, they had to spend significant time figuring out how to keep the username-only system while making it reasonably safe. They eventually implemented the QR code system that wasn't there initially, where you have to scan a QR code to log in. This prevents someone from sending you a login request that you accidentally approve. They also added the ability to change your username directly in the app, which wasn't possible before.

When we initially reported this issue just days after launch, they responded that they had sophisticated systems to prevent exploitation at scale, so we shouldn't worry about it. This put me in a dilemma because they were essentially saying "prove it," but if I actually did that by blocking multiple usernames, they would likely sue me for attacking their servers.

A year later, a journalist contacted us wanting to prove this vulnerability, so I provided some code, and after that demonstration, they finally changed it. However, they still claimed they had known about this issue all along and were already planning to change it.

One of the biggest issues is that there's still no official way to report security issues to Digitaliseringsstyrelsen. As of at least six months ago, they still did not have a dedicated security incident email. You have to go through customer service and say you have a security issue to report, and they'll either put you in contact with someone or just tell you to write it to them directly. That's not appropriate for handling security vulnerabilities.

They're completely reliant on people's goodwill, as I could have potentially sold some of the information I found to someone willing to pay more than the Danish government, which pays nothing. When you don't pay anything and treat the people helping you as if they're a problem rather than a help, you risk someone eventually deciding to sell vulnerabilities to parties who will pay for them.

Interviewer: How has Denmark's digitalization strategy influenced national cybersecurity, particularly in crucial sectors like healthcare and finance?

Expert: My insight is limited since I haven't worked in these agencies, but from what I've seen with MitID, what's being built isn't bad. There are people who care, and they're hiring consultants who build good systems. Security is being taken into consideration.

However, from a security researcher's perspective, they don't respect our input nearly as much as the private industry does. They make it difficult to be a security researcher who wants to help the government. There's not much adherence to the standard rules you generally follow in security research.

Interviewer: What are the main security challenges associated with MitID, and how does it compare to previous authentication methods like NemID?

Expert: The underlying algorithms are almost the same—they've been updated a bit, but it's basically the same code with a new frontend. The MitID we have today is much better than when NemID was phased out, but there was a bad period during the migration. They should have been more receptive to feedback when they first released it, as that's when feedback is most needed.

With NemID, the biggest problem was social engineering. Someone could send you a photo of the key card, or if they knew when you were logging in, they could send you a request that you might approve, logging them in. This is nearly impossible with current MitID unless you use specialized tools.

The QR codes are now valid for only 20 seconds. They're not static—there are two QR codes constantly swapping every 10 seconds, and after 20 seconds any QR code becomes invalid. This means if someone wanted to scam you, they would need to send you a video of the QR code that you need to scan within 20 seconds, which is very difficult to achieve in a social engineering attack.

I've actually built a Python client that does exactly what the real MitID browser software does—it creates a login request with a username and generates the QR code as a video file. If this were integrated into a website, you could theoretically create a phishing site, but I haven't seen anyone do that yet.

The problem is that in a web environment where anyone can participate, it's almost always possible to create fake versions of websites if you're willing to spend enough time. But generally, MitID today is very strong, especially in protecting against social engineering. They've done a serious job of making it increasingly difficult to exploit.

Interviewer: How would you comment on the identity theft issue comparing NemID and MitID?

Expert: With NemID, if I knew your CPR number and password (which wasn't always easy but wasn't impossible), I could send you a login request and then call you—especially if you were elderly—saying, "Read me the code on your card" or "Swipe to approve so I can help you," and they might comply.

With early MitID, this was still possible, but today it's much harder because of the QR code requirement. You'd have to send them a valid QR code with only a 20-second window, which makes social engineering attacks much more difficult. An elderly person wouldn't understand how to use such a complex attack vector.

There's also a small code reader available as a backup that generates a six-digit code. The authentication flow requires you to enter the username, then the six-digit code, and then the password. This means an attacker would need to know both the username and password before even attempting to get the six-digit token from you, making it very difficult to execute an attack.

I think MitID is very well designed; I just wish they were more receptive to outside help.

Interviewer: What lessons can be learned from international cyber incidents to further enhance the security of Denmark's digital identity infrastructure?

Expert: When I see international incidents like the major Social Security number leaks in the US, they typically involve systems of much lower complexity than the Danish MitID system. I think we are at the forefront. I can't recall seeing a system as sophisticated as MitID being compromised.

Our system requires an attacker to know something, be somewhere, or be someone specific—it's a very tight system. Of course, there's always the risk of someone introducing a coding bug that allows unauthorized access, but if it works as designed, it's quite secure.

Interviewer: How do you see the future of Denmark's digital infrastructure evolving, both realistically and ideally?

Expert: Realistically, I think we will continue to be at the forefront of technology, especially with identity-based systems where we excel. But we'll also remain secretive about how it works and continue paying private companies to implement it without developing in-house expertise.

Ideally, I would like to see the government hire experts with significant expertise in what they're actually running. I'd also like more transparency about how these systems work. By being more open, we could identify more issues.

When reverse engineering the app, I found an API endpoint that was only used in the app—not documented anywhere. This endpoint allowed querying usernames without the rate limits that were applied elsewhere. They were relying on security through obscurity, thinking no one would find it because it wasn't documented. By making systems public and transparent, you put more pressure on every part of the system to be secure.

I'd like to see the Danish government make some of these systems open source. The point of moving to MitID was that it would be state-owned, but they're still paying private companies to run it. In my experience, these companies were the only ones who understood how it worked, and they weren't interested in open-sourcing it—possibly because they wanted to sell similar systems to other states or companies. The government officials, lacking technical knowledge, were inclined to believe these consultants when they advised against open-sourcing.

Interviewer: Which cybersecurity measures should be prioritized to mitigate emerging threats?

Expert: I would like to see the government implement a bug bounty program. I don't really care that I didn't get paid for what I did, but having a program where they pay for security vulnerabilities would incentivize responsible disclosure.

At minimum, they need proper contact points for security issues and people who know how to handle them—people who don't panic when presented with security issues and understand you're trying to help. They should understand you didn't have to report the issue and appreciate that you did.

Typically in security research, you might say, "I found this vulnerability and would like to release it in 90 days. Do you have any reason why I shouldn't?" But the response is often just, "You have to wait," without any timeline or explanation.

Interviewer: How do you envision the ideal model for a bug bounty program and security reporting system?

Expert: The ideal outcome might be a centralized portal serving all Danish agencies where you can submit security issues and specify which agencies are affected. The government is in a unique position to have a single portal for all government systems, which could ensure reports are handled correctly.

Regarding bounties, this is standard practice in companies. Especially with ongoing international conflicts, it's more important than ever to ensure there's not only profit to be made by those with malicious intent. Right now, the ability to compromise MitID might be valuable to certain adversaries, but the Danish government doesn't place any monetary value on that information.

Interviewer: What are the main threats to Denmark's digital infrastructure?

Expert: I'm no expert, but the main threat is Russia. They have the most interest in causing harm. China might have some interest, but I don't think they have nearly the same motivation.

Interviewer: Thank you for your time.

Expert: I hope you got something useful. I'm by no means an expert in this field, but I have some unique experiences with the government agencies.

Interviewer: Can I contact you again if needed?

Expert: Absolutely. I'll also be at ICU on the 7th of March to do a 30-minute guest lecture on MitID reverse engineering.

Interviewer: If you prepare a presentation, could you please send it over? Also, may I use information from your thesis?

Expert: Yes, once I've completed it, I'll send you the presentation. And absolutely, the thesis is public knowledge so you can use all of that information as far as I'm concerned. It's interesting because it shows some of the issues that existed before that have now been fixed, demonstrating improvements in security.

Interviewer: Thank you very much for participating in my interview.

Expert: No problem. Good luck!