PCU

Personal secure
Cyber-biologic
Universal identification unit

Protect your biological data and secure your digital life with a PCU

- Third generation Digital ID for personal security

Going from passwords to a secure Digital ID

- The first generation of digital security, using passwords, codes and user names, has obvious weaknesses, and is therefore gradually being replaced by new technologies.
- The second generation of digital security, now rapidly gaining ground, uses biological data, thereby creating a new risk for its users; having their real biological data stolen.
- The Third generation of digital security also uses biological data, but in such a way that there is no danger of losing the actual data. This is where PCU comes in.

PCU ensures personal security by using Cyber Biologic ID, CB-ID

A Cyber ID is generated using a mechanical, production technical solution and real biological data to form a unique Cyber Biologic ID, CB-ID. This gives a unique personal identification method where your real biological data can neither be recreated nor stolen The Cyber ID is generated in a PCU, which can either be a freestanding unit or an integrated part of a mobile phone. The PCU transmits the unique ID and reads your biological data without storing them. Losing the unit is therefore not a problem, as no biological data are there to be revealed, and the unit can easily be replaced, giving you a new unique Cyber Biological ID, CB-ID.

• A Cyber Biologic ID, CB-ID, is a personal, unique and replaceable Digital ID

- PCU is a patented solution with a multitude of unique security features suitable for all users.
- PCU offers scalable security levels ranging from simple solutions for your car to more advanced systems for banking and financing

PCUcompany.com

PCUcompany.com

Securing it all

What is a PCU?

A PCU is a **Cyber Biological Identification Unit** that communicates with everything from door locks to login solutions for PC's or Internet banking. It is easy to bring along wherever you go, either as a small, separate unit replacing keys, access cards, pin code devices etc., or as an independent unit integrated in a mobile phone.

How does a PCU work?

Forget passwords, keys and codes. Choose your own method of identification, using biological properties such as **iris, finger print, facial** or **voice recognition**.

Instead of using your actual biometric data, the PCU will generate a **Cyber Biologic ID** (**CB-ID**) for authentication. As with your real data, this ID is not stored in the unit. A PCU will give unique CB-ID's for every individual user at all times.

The PCU uses industry standard technology to communicate with systems such as Bluetooth, NFC, Proximity, WiFi and 4G.

What can a PCU be used for?

A PCU **can be used for nearly all** digital units demanding secure access. Many web-based services and systems have no need for identifying a person, but merely require an authorized user. A PCU can be used for **authorization as well as and identification**. The unit can also be used for other purposes, such as locking your house or car.

Why PCU?

There is a large and ever increasing number of solutions for logging on to various systems, opening doors, paying or transferring money etc., and each of these solutions require their own code and password. However, the level of security that these passwords and codes are meant to uphold is compromised when the user has one password for all user accounts, or makes notes of the accounts with corresponding password or code. The need for **one simple and secure standardized solution** is therefore rapidly increasing.

This standardized solution MUST be a secure option, and as opposed to an app or a password, the PCU is precisely that.

Why is the PCU secure?

The PCU addresses two important issues relating to security and safety. Firstly, to ensure that **only the right user is given access**. Using biometrics is a much safer option than using a PIN and password. The PCU utilizes a unique biometric solution CB-ID, always send and handled by encrypted communication only, and state-of-the-art security technology.

Secondly, the PCU addresses the danger attached to applying biometrics. The use of finger prints etc. is rapidly increasing, but the risks are rarely mentioned. If you lose a PIN code or password, you can get new ones. **If you lose all your biometric features, they cannot be replaced**. The PCU ensures this will never happen by neither storing nor sending real biometric data – it merely utilizes the best of both, being exact and replaceable. Having a user's Cyber Biometric data is not enough in itself; you also need the right PCU. In addition, a lost CB-ID can easily be replaced.

The dangers of losing your real biometric data or your CB-ID are therefore reduced to a minimum.

How will the PCU succeed?

The PCU will succeed by obtaining a «**critical mass**» of users. When you reach a level where enough people are using PCU in one area, the interest will spread into other areas. This will in turn attract more users, and open up even more areas for using the PCU.

Examples of such areas are banking and financing, door locks and access control, access to public sites, equipment manufacturers (smart phones, PC's, cars), social media and Internet and general communication.

How can the PCU solution be organized?

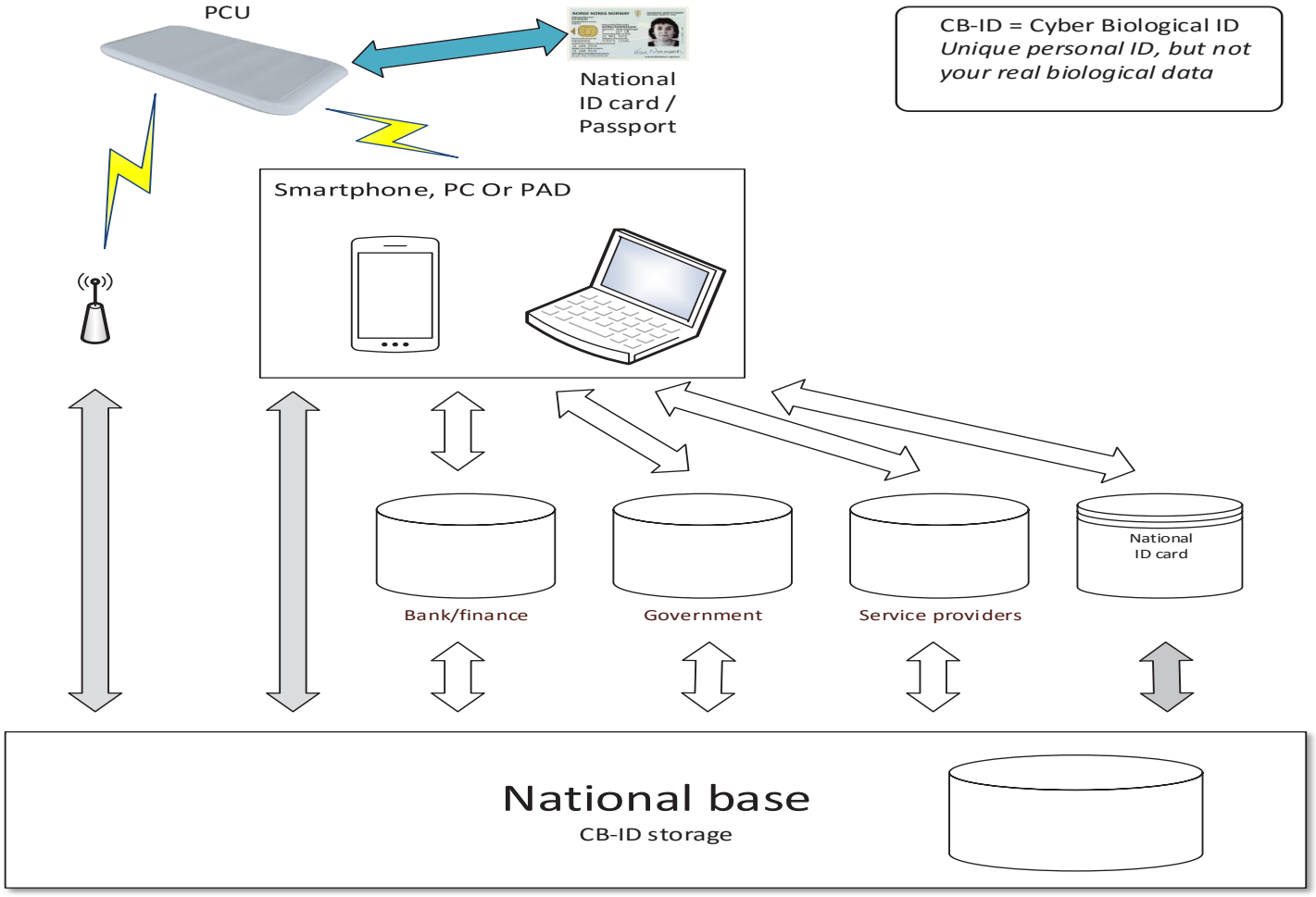
It is possible to use the PCU in a limited area only. However, the strength of the product as a universal solution using the best mobile technology is enhanced as the number of usage areas increases. With a multitude of applications it is possible to establish a **central management** of the overall solution, while the individual PCU's are still used in clearly limited areas.

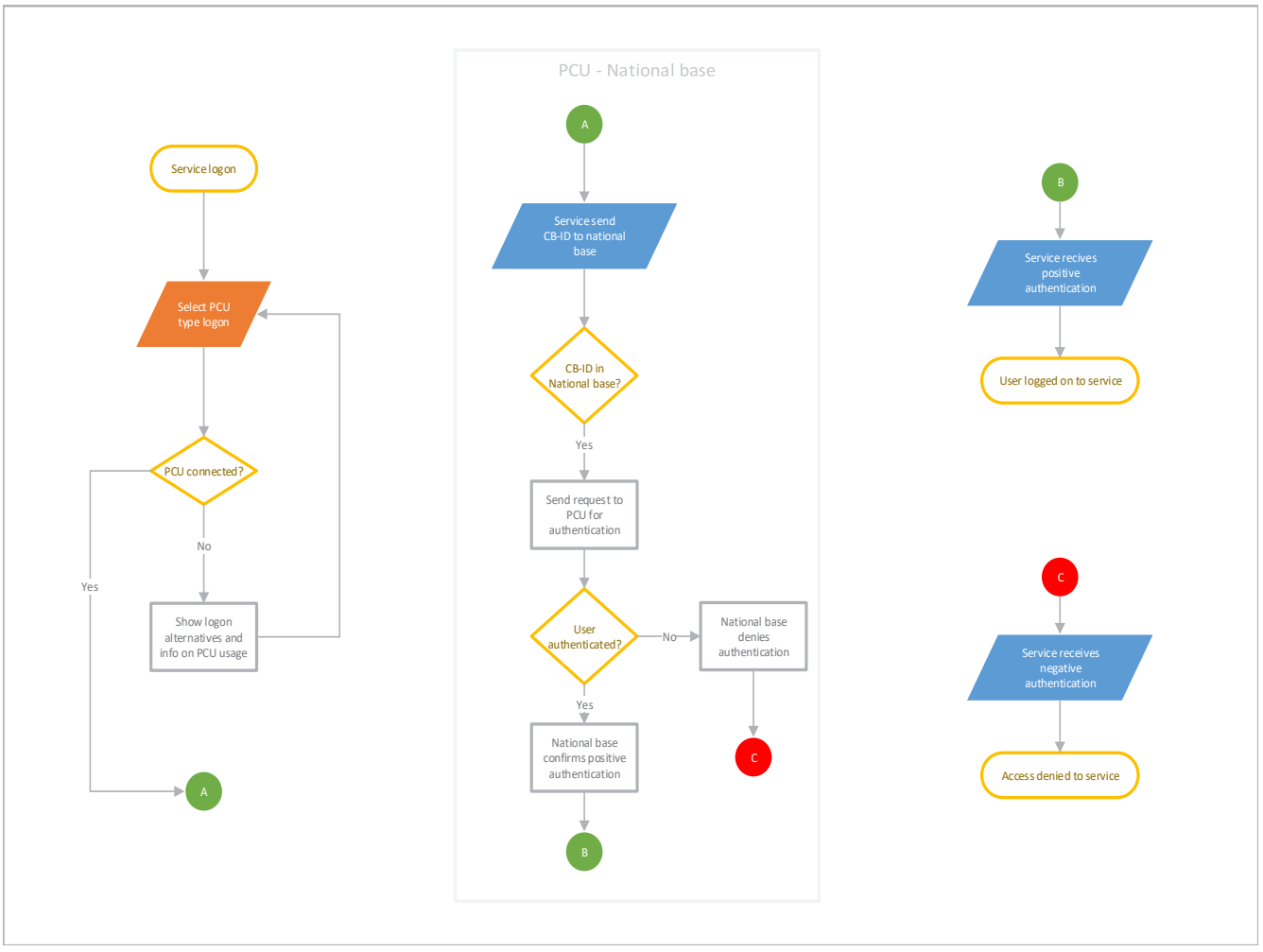
A future prospect includes **a national database** with sub-groups for central management within banking (e.g. mCash, Vipps, Swich, MobilePay, Internet banking and trade) and the public sector (e.g. tax and business reporting services (Altinn), the Inland Revenue Service, the Norwegian Labour and Welfare Administration (NAV), National ID cards, passports, driver license)

How to survive in an insecure digital future

- **Never store real biological data** (not even when encrypted)
  Lost real biological data can never be regained or replaced.
- **Use only Cyber-Biological ID's** (CB-ID's) and make sure these are stored in an encrypted form, and not in the PCU.
- Use only CB-ID type identifications as it is easily replaced by reading a CB-ID from a new PCU or loading a new biometric combination from the existing PCU. A person can have several active CB-ID's when using more than one PCU.
- If a PCU is lost, your stored CB-ID can easily be blocked in central databases, and stolen CB-ID's will not work when a compromised CB-ID has been replaced.

PCU Company – aiming to be best, not first!


PCU
National
ID card /
Passport
CB-ID = Cyber Biological ID
Unique personal ID, but not
your real biological data
Smartphone, PC Or PAD
Bank/finance
Government
Service providers
National
ID card
National base
CB-ID storage


Service logon
Select PCU
type logon
PCU connected?
No
Yes
Show logon
alternatives and
info on PCU usage
A
PCU - National base
A
Service send
CB-ID to national
base
CB-ID in
National base?
Yes
Send request to
PCU for
authentication
User
authenticated?
No
National base
denies
authentication
C
Yes
National base
confirms positive
authentication
B
B
Service recives
positive
authentication
User logged on to service
C
Service receives
negative
authentication
Access denied to service

Innovation Norway supports PCU Company

Innovation Norway has decided to support PCU Company, both in terms of professional guidance, and also with funding in the «Marketing Planning Phase». This has given us a solid foundation to continue our activities, and has paved the way to success for us as a newly established company based on eight years of active research and development, resulting in a secure Cyber-Biological Universal Personal Identification solution. A PCU Cyber ID (CB-ID) is suitable for all persons who need accurate personal identification, but wish to protect their real biological data from hackers and criminals.

Egil Henning Ytrøy in Innovation Norway was quick to approve support to the marketing planning process for PCU Company, and has contributed with valuable advice and guidance along the way. This has enabled us to produce the necessary tools, brochures, web pages and presentations required to initiate communication with important and knowledgeable contacts in many leading Norwegian businesses and companies within banking, IT and public administration.

PCU Company – aiming to provide order in the chaos of mobile payments

A Personal Secure Digital ID is the common denominator which may provide much needed order in the chaos of mobile payments. PCU Company's analysis of several hundred market actors revealed the same trend in Norway, as World Economic Forum has uncovered in their new analyses worldwide. Both reports show that mobile payment systems are diversified without any common direction. (WEF's new report on disruptive innovation in wireless digital Financial Services is called the «Blueprint for Digital Identity».)

According to both these surveys, the old and well organized collective payment solutions, national

ID, bank ID and trade solutions, which used to work everywhere, are substituted by new solutions lacking any unified structure. In less than a year, a vast number of new solutions have been introduced in the market, creating chaos and confusion for both commercial actors and their customers. Vipps, mCash, Swich, MobilePay, ApplePay, AlibabaPay, Paypal, GoogelPay etc. are all nice and temptingly easy, but much more expensive to use, and require several types of point of sale (POS) terminals in each shop.

This chaotic situation has scared Norway's major retailers into forming an expert, specialized, company working to develop a common solution for wireless POS payment that is simple and reasonable to use with all types of mobile apps; Retail Payment AS.

Banks have been busy trying to attract young customers with fun and easy solutions on the mobile, while at the same time making life more difficult for others.

By standardizing on a PCU CB-ID solution, the banks will be able to coordinate their own systems with NFC payment on most existing POS terminals. And if the payments are routed via local payment partners such as BankAxept and NETS, great savings can be made. This is important to prevent a situation where some banks and traders have to shift today's high level of costs onto the customers. Mobile payment is so far free of charge to the customer, leaving the banks to pay the bill from foreign payment partners such as Visa and MasterCard.

The PCU solution can simplify and secure payments for everyone, while at the same time protecting real biological data from hackers and criminals. With a Personal Secure CB-ID, both banks and public authorities can settle on one common standard for both payment and accesses with the CB-ID as customer ID, as well as common registration in their databases.

Putting personal security first is the only way forward

Putting personal security first by securing the users' biological data is the only way to go for both banks and national database solutions. Everything connected online is at risk of being hacked; therefore everyone in need of safe digital identification has to use a Personal Secure Identification method, such as a PCU type solution.

Only companies who focus on individual personal safety, offering a free selection of services, will succeed in spreading their solutions to a wide audience. The whole world embraced the personal bank card for both debit and credit payments. When IBM introduced the *Personal Computer (the PC)*, the individual use of computers exploded worldwide. The personal free Internet was an instant success. The same may be said for the personal phone; nowadays everyone has their own mobile. Facebook's enormous success can be attributed to the fact that they *focused on the individual person* with a free *personal choice* of friends.

Digital-ID, Bank ID and Public ID of the future can only gain ground with a personal safe and secure solution offering freedom of choice for everyone – no matter who they are or where they are.

PCU Company is using eight years of research and development to create an accurate and personal secure Cyber-Biological Universal Identification, CB-ID, without compromising the user's real biological data. We will cooperate with major actors in various business segments to disclose needs and specifications, with an aim to produce PCU solutions for accurate and personal safe identification of users in all segments.

A targeted effort from PCU Company to create solutions covering every need will require significant public support for production and internationalization. In addition, we need further support from heavy, long-term investors. Who wants to join us on our digital quest to provide secure personal identification for everyone?

Your future Personal Secure Cyber-Biological Universal Identification, CB-ID solution, PCU, is patented in 40 countries, including China, Hong Kong, Canada, Scandinavia and the whole of the EU to ensure a uniform and homogenous development.

Guest Commentary: Harald Marthinussen, Civil Engineer, PCU Company AS

Too many passwords and codes

With smart banking solutions like DNB's Vipps, surely, the need for passwords and codes will be eliminated? Yes, it must, because the way it is for most people today, passwords provide false or no protection towards losing your identity and valuables. The use of passwords and codes have become a problem, and hopefully, soon a thing of the past.

On average, we have to memorize 20 to 30 user names, passwords and access codes. But do your really remember all your passwords, codes and user names for G+, One Drive, Twitter, PayPal, MasterCard, Visa, Amex, Shell card, Statoil card, PC/PAD/Smart phone, Facebook, LinkedIn, Instagram, Social Security, tax return, Internet bank, online health journal, cloud storage, company server, passport, bank card, home front door, workplace access, etc., etc.? Relax, neither do the rest of us.

Most people need to keep a list in their purse or wallet, unless they store all these codes in a password organizer on their PC or smart phone, or simply use the same code for everything, varying perhaps the first and last digits. Or maybe you are the type who leaves ID cards and codes for accounts, payments and taxes to your accountant or the family economist?

All this makes the new digital world extremely dangerous to everyone involved, not least to employers. It comes as no surprise that the US public authorities have been hacked, thereby losing the biometric data of a great number of employees. The hackers also gained access to social security files containing classified information. American authorities admit that they have been robbed of 5.6 million sets of fingerprints, as well as 21.5 million classified «victim SF-86 forms» and «security clearance questionnaires» containing personal information on issues such as previous drug abuse and family affairs. Now, all this information can be used for both threats and blackmailing purposes.

The major credit card companies have declared that plastic cards and codes will be replaced by wireless person identification using gadgets or jewelry, while at the same time, the banks are competing in finding even more complex solutions for passwords, codes and mobile ID's. The world has become a strange place when one hand has no idea of what the other is doing.

The Norwegian banking system must further develop its solutions for improved security, and make them more understandable to ordinary people. Secure solutions for personal identification supported by voice-controlled communication in people's own language, will make the process comprehensible, even for those who are struggling to keep up with the technological development. This allows you to speak normally with digitally controlled doors, PC's, cars, banks, POS terminals, workplace access controls and online services, often through a mobile phone, which requires a secure identification before you receive the goods or services you need. A common Norwegian «voice-controlled NETS», or perhaps one for the whole of the EU, will allow standardization and simplification of all bank services. Bankaxept and BITS (Norwegian banks' common standardization office) should be able to organize and set this up in consultation with their partners, e.g. Visa, MasterCard, Eurocard, Amex etc.

So when will passwords and codes become a thing of the past? By studying the development rate of the voice assistants Siri, Maluuba, Alexia, Cortana or Robin, and the final development of a common, 100% secure cyber-biological authentication solution, it is possible to predict that it will take from four to ten years before passwords and codes can be permanently phased out. This also depends on Google, Microsoft and Apple giving priority to the development of voice assistants, which must be linked with copy secure search engine services to create a safe and simple world without ID's, codes and passwords.

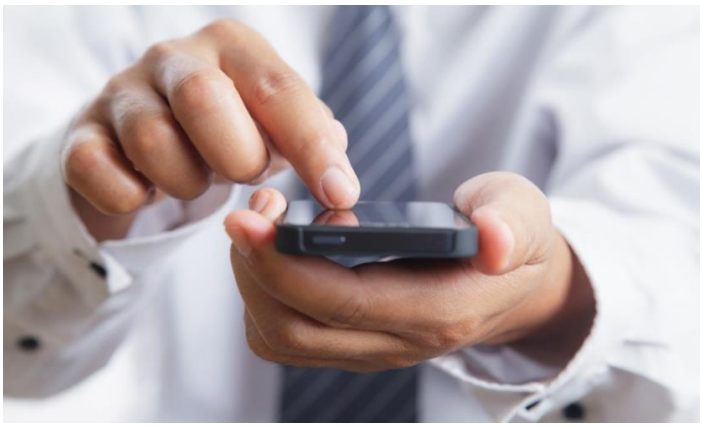
In a new digital world, the only feasible solution is a combination of man, technology and software. Oral communication, quick searches in copy secured databases and accurate personal identification, not possible only a couple of years ago may become the future before we now it.

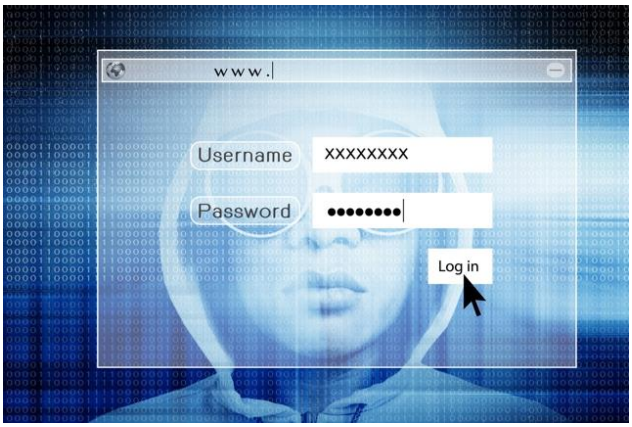
[Translated from article published I Kapital 3/2016]

Biological Bank ID can be potentially deadly | ABC Nyheter (ABC News)

Thursday August 4, 2016

We are not only running the risk of being robbed of money, our biological data may also be stolen.





Civil Engineer Harald Marthinussen is wary of the fact that in future, we may have to identify ourselves using our real biological data, for example our finger prints. In February, The Norwegian Center for Information Security (NorSIS) reported that 150,000 Norwegians had been a victim of identity theft in the last two years. Photo: Colourbox.

Every single day, we log on to a two-digit number of apps and web sites, using passwords, personal identity numbers, code devices or codes. This first generation of digital ID methods is now gradually being replaced by other solutions.

In future, you will identify yourself online using real biological data. For example, when logging on to the Inland Revenue Service or other tax and business reporting services such as Altinn, you will have to reveal your biological ID in a mobile app, using either your finger prints, the sound of your voice or a selfie. You will then be automatically logged in, without entering a code.

This technology comes with a risk: You may suffer a premature «digital death» if your biological ID is stolen.

Just recently, Mastercard has made it possible in 17 countries to approve mobile payments by taking a selfie with your mobile. They will also use everything from fingerprints to voice recognition to offer the safest way of identifying the person paying – without considering the implications of biological identification. This should worry us. Not only do we risk losing money, which Mastercard will have to compensate us for, we are also running the risk of letting our biological data getting into the wrong hands.

Microsoft is another major actor going away from passwords and codes by using biological ID methods in the new Windows 10. This trend will become more and more prevalent in the years to come. We are already having problems securing our digital identity with all the information we need to remember. On average, every single one of us has to remember 20 to 30 user names, passwords and access codes. And only a select few can truthfully say they have the memory this takes. Most of us have to write down the codes, e.g. in a password organizer on the mobile – or simply use the same code for everything.

Passwords stored on your mobile can be stolen. 150,000 Norwegians have been victims of ID theft, and in the United States, the classified documents of 21.5 million public servants were recently stolen. The conclusion to be drawn from this is that no databases are 100 % secure. And neither are mobile phones.

The world leading technology web site TechCrunch was hacked by the same group that assumed responsibility for breaking into Mark Zuckerberg's Facebook and Twitter accounts, and making the

«Pokémon Go» servers come to a grinding halt. This only goes to show that even the best cannot escape the threat of hackers.

We are drowning in a sea of life-critical apps – which we cannot even find in life-threatening situations

Within 2018, at least 50 per cent of us will use the mobile for most everyday tasks. The mobile phone will literally open doors. It will give access to trains, museums, cinemas, and your workplace. You will pay for drinks, withdraw cash and pay private debt using the mobile – while at the same time sharing a lot of this information with other people's mobiles.

Having to use so many apps also poses a personal safety problem. Since 2008, 1.5 million new apps have been introduced to the market. Most mobile users have more than 20 apps stored on their phones, and use four to six of them daily. In other words, we are drowning in a sea of «life-critical» apps we will not even be able to find when faced with a life-threatening situation.

In Europe, nearly 1,640,000 people work in the app industry. Norway has Europe's second largest app industry seen in relation to its number of inhabitants, with 41,000 employees working on new apps every day. The great number of apps compromises the security of our digital ID even more.

Many of these apps are now starting to use biological identification. A clever hacker can steal anything from your mobile phone, even if it is locked with a code – and even if the information is encrypted. Recent reports say that American authorities purchased solutions from hackers to be able to break into the iPhone of the killer in San Bernadino.

When American authorities so easily can buy this type of tools, how do we know that IS, Mossad, al-Qaida, Iran, North-Korea or common criminals are not doing the same?

Everything you do on a mobile phone can be stored, leaving it open to theft and hacking, and making the security of the phone very poor. Photo: Colourbox

Can the entire population become digitally dead to Google and MasterCard?

You are putting your biological data at risk if you, like many iPhone users, have registered your fingerprint on your mobile. In one of their technical seminars, Google demonstrated that they were able to identify the drivers of cars passing a roadside camera by comparing their faces to all the faces in their global data storage facilities.

Norwegian authorities save and store your picture and fingerprint whenever you renew your passport. **If the Norwegian national, public databases are hacked as they were in the US, and the personal data of 5.6 million people, including facial photos and digital fingerprints, are stolen, we are not only digitally dead when it comes to using the recorded fingerprints. We can also become digitally dead to both MasterCard's «selfie payment», as well as to Google's facial recognition.**

Biological Bank ID can be potentially deadly | ABC Nyheter (ABC News)

But as opposed to a username or password, your fingerprint or face cannot be replaced. If the publicly stored passport information gets into the wrong hands, this may cause the digital end of a whole nation.

Can biological national and bank ID cause a premature «digital death» for you?

As we usually trust banks, credit card companies and public authorities to secure our valuables, the resistance towards using biological ID will not be noticeable until a sufficient number of people have had their fingers burnt by losing vital biological identities forever. It took 15 years before many enough had felt the effects of careless handling of viruses. Compared to this, it will take only two years before today's introduction of biological ID will have to be replaced by more personally safe, cyber- biological, universal reading solutions.

We have to use Cyber Biologic ID Readers, CB-ID Readers, as «simulated copies » of your biological identities, e.g. cyber eye-iris, cyber fingerprint, cyber face (selfie) and cyber voice recognition. The CB-ID Readers must be small, portable, self-contained smart units offering the user a choice of which CB-ID to use for different services.

A Personal secure Cyber biologic Universal portable reader – a PCU – must, unlike all other readers in today's mobiles, PC's and gadgets, be cleared after each identification, so that nobody can access your personal cyber data if the unit is stolen or hacked. This will prevent hackers from using biological fingerprints to steal people's personal data from millions of smart phones in the near future.

According to Harald Marthinussen, being personally in control of how to safeguard oneself against future identity theft is the only way forward in a complicated digital future. Photo: Private.

Personal Secure control of our own identity is the only solution

Data processing and electronic communication did not become a general success until the PC entered the scene in the 1980s, and the Internet put the individual person in the spotlight during the 1990s.

Being personally in control of how you wish to safeguard yourself against future identity theft is the only solution for an otherwise complicated digital future. Your own personal, portable and unique CB-ID ensures that your real biological data are not misused by banks, credit card companies, public authorities, or other suppliers with strict identification requirements.

The personal CB-ID conceals your real biological data, giving you both an easy and accurate identification method, as well as far better protection against hacking in existing and future solutions. This is achieved by securing and encrypting scanned data with anti-cyber attack software, and 256 bit or higher TM or AES type encryption using a 12-digit production number. Leading Nordic patents from companies such as Idex, Next Biometric, Zwip, Fingerprint and PCU Company can be utilized in combination with solutions from Mcash, MobilePay, Vipps and Get-swish to create the best solutions for the future of Personal CB-ID.

Nordic inventions, patented back in 2012 in 40 countries including China, Hong Kong, USA, EU and Canada, should be able to secure our future within two years.

Both Google and credit card companies like Visa, Mastercard and Amex agree that plastic cards, codes and passwords will soon be replaced by smart little units encased in a piece of jewelry or a small gadget holding your Cyber Biologic ID readers. **Every person's Cyber Biologic ID is unique and individual, but is not identical to your real biological data. Therefore, a CB-ID can be replaced if stolen, and your digital life can always be renewed – allowing you to emerge as a whole new cyber person ready to move on with your life.**

Guest Commentary: Harald Marthinussen, Civil Engineer, PCU Company AS

Your Digital Butler

Are mobile payments with and without Bank ID a safe option? Or are they downright deadly?

The use of mobile phones has exploded. The mobile – our new PC – involves a whole new set of security requirements for everything and everyone. All mobiles need extra security to ensure a safe connection for your data to be protected against unauthorized access and misuse.

New statistics from market analysis bureau Gartner's show a strong increase in the sale of mobile phones, reaching 1.9 billion units in 2015. This means that pretty soon, everyone will own a mobile phone, including people in most poor countries. They come in the form of car computers and laptops, and are connected to the Internet through free-standing IP addresses that are not protected by the firewalls and security systems at your employer or in your home. This creates huge security risks all over, without new requirements for secure identification of users whenever they are as terminals connected to their workplace or for secure services online.

Mobile phones open doors and grant access to trains, museums and offices, as well as various arenas for recreation and sports. You pay for drinks, withdraw cash and make down payments on private debt through the mobile phone without the necessary security. All this is done by sending different unsecure personal ID's and Bank ID's from your mobile. You can even send your digital keys for your home, office or car to your cleaner, mechanic or friend, so that they can open your doors with their own phone.

Anything you store on a mobile or a PC connected to the Internet, can and will be stolen by criminal hackers. One day, your personal identity will get into the wrong hands, including your biological data stored on your iPhone 7S, Lumia 950XL, Galaxy 7S, Xperia z, etc. When this happens, you've had it – for good.

When you use voice-controlled assistants such as Siri, anyone with a certain level of computer skills can steal all information stored in your phone, e.g. names, addresses, phone numbers, e-mail addresses, photos, messages and classified information, even when the phone is locked with a code. It will happen sooner or later, and when it does, you had better be prepared by securing important data using «end-point security» for access and connection to everything of value to you, your family and your employer.

Mobile phones are also traced on Facebook, GPS and Google, so that commercial advertisers, competitors and criminals can follow your every step through your use of the social media. However, you can keep your customer visits, trade transactions and travels to yourself by using your own, personal CB-ID, sent from your secure personal smart key for everything you find important and choose to protect.

Can the future be simple, pleasant and safe for everyone? The answer is yes. New inventions and solutions are being developed all the time. For example, when finished, solutions such as Siri, PCU, Maluuba, Cortana, and personally controlled cyber-biological authentication systems will render all your passwords, user names, ID's and many of the mostly used apps, completely superfluous.

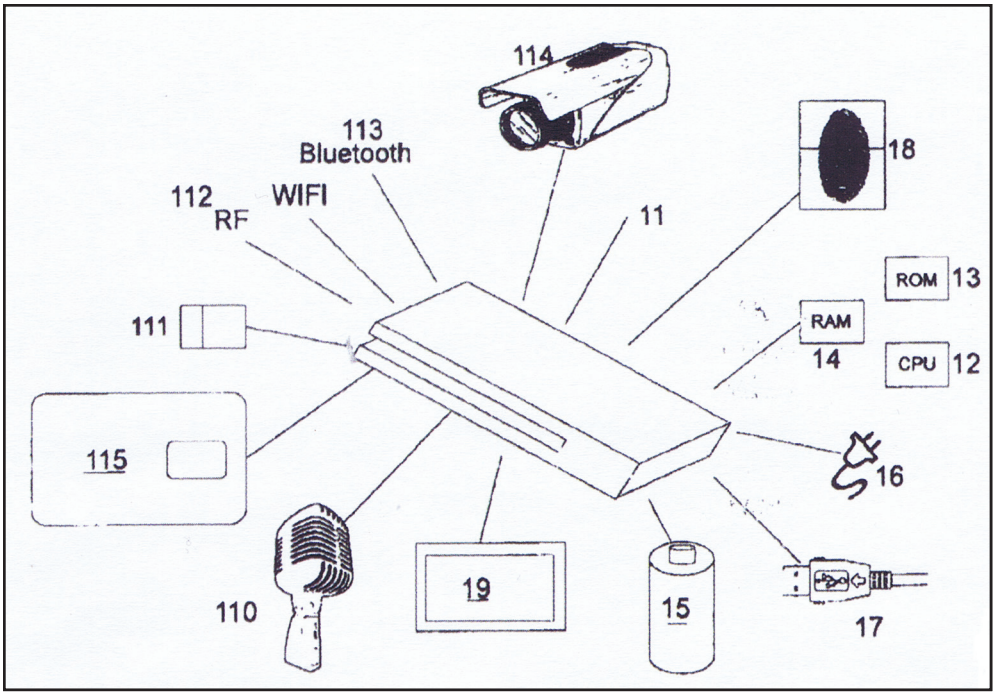
Instead, you will be able to talk to a voice-controlled assistant; asking the bank to pay a given amount, requesting the opening of a website through Google, getting insight into your registered VAT and tax, or gaining access to your online stock trading transactions. All this will happen when you are identified by your cyber-biological identification unit, with your own chosen CB-ID.

You will be talking to your pleasant voice-controlled assistant as if he were your digital «Cyberspace Butler», who both recognizes and understands you without being physically present. This is just how simple life can be without compromising the security of your person or your valuables. We must remember that in a new digital world, the only way forward is using a combination of human choices, custom-made technological solutions and secure programmable information databases with Big Data. Oral communication, personally selected security features, quick searches in copy secured databases and accurate personal identification – not possible only a couple of years ago – may become smart solutions in the very near future.

Good luck in a fun, convenient and enjoyable future, assuming it will come sooner rather than later.

[Translated from article published I Kapital 7/2016]

Norwegian patent will prevent car hacking - Digi.no



Norwegian inventor Harald Marthinussen has given it the name Personal Connection Unit (PCU).

The PCU is a wireless identification unit which works as a connecting link between the user and any electronic device, such as your car, iPad, bank card or door lock.

The summer 2015 his patents was approved in 40 countries.

No more pin and password

– This unit will replace pin codes, user names, passwords, keys and access cards, explains Civil Engineer Marthinussen.

He runs an IT company called KK88 in the town of Ski just south of Oslo, and has a colourful CV with highlights such as working with research and development of space travel solutions for American companies linked with NASA's Apollo project

Civil Engineer Harald Marthinussen has patented his electronic identifier, which is designed to replace pin codes and passwords – and make stolen passports worthless. Photo: Pressefoto.

High level of security

The principle behind the PCU is to have a battery powered unit that is unique to each user, but useless to anyone else.

It registers biometrical data, such as iris patterns or fingerprints, to allow access for the user by activating Bluetooth or NFC frequencies to make contact with the targeted unit. When higher security levels are needed, the biometrics is combined with crypto solutions.

– At a lower security level, the PCU only needs to be near the connected unit in order to respond, e.g. opening a garage door simply by approaching it, says Marthinussen

Stop car hacking

Our aim is to start mass production of the unit for use in sectors such as general industry, transport, healthcare and private applications.

Inventor Marthinussen gives us an illustrating example:

Just image that you have to keep the unit in your pocket, close to the ignition, in order to start the car. The PCU has an operating range of 30 cm. Therefore, if someone is trying to hack a driverless car, you can simply throw the unit into the back seat; the car will lose its “clearance” and the engine stops.

He also predicts that some time in the future, the unit can be linked with all passports. A passport will not be active and cannot be verified without the PCU.

This will make all stolen passports worthless, states Marthinussen.

Theft

- But what if the unit is stolen?

The unit only works together with one person’s biometric values, and is useless to everyone else. It is not connected to the Internet, and can therefore not be hacked. In addition, hacking the unit is of no value to anyone, as the approved login data are deleted as soon as they have been used. The PCU has no storage capacity, replies Marthinussen.

- Do you think people are willing to bring another gadget along with them everywhere, in addition to their mobiles?

Our plan is to design different versions, including a PCU that can be placed in a slot on the back of the mobile. This ensures regular charging, but there is no data connection.

Funding

So far, the inventor has tested the PCU in an unfinished design, which he does not wish to display to the public.

He reckons it will take several months to finalize the design.

Right now, we are mapping the requirements and specifications of more than 100 areas of application. At the same time, we are working on modulating several different sizes to test factors such as grip and finger size, in order to find the right specifications for the ultimate user-friendliness, explains Marthinussen.

He is now looking for funding to finance the production of test units for live testing of the PCU.

We need a large number of units to carry out extensive final tests in more than 500 areas of application before the mass production can begin. The tasks ahead of us are many and large, and may take a very long time if we do not find partners to help us pull this together, says Harald Marthinussen.

In total, we need approx. NOK 120 million to build an organization that can handle various product areas such as transport and finance, on an international level.

Espen Zachariassen – Digi 4. Aug. 2015

Guest Commentary: Harald Marthinussen, Chairman of the Board, PCU Company

The war of mobile payments has started

Who can provide order in the chaos of mobile payments without putting personal security first?

A Personal Secure Digital ID is the common denominator which may provide much needed order in the chaos of mobile payments. PCU Company's analysis of several hundred market actors revealed the same trend in Norway, as World Economic Forum uncovered in their «Blueprint for Digital Identity». Both reports show that the old and well organized collective payment solutions, national ID, bank ID and trade solutions, which used to work everywhere, are being replaced by new solutions developing in all directions, with no unified structure.

In less than a year, a large number of new solutions have been introduced in the market, creating chaos and confusion for both commercial actors and their customers. Vipps, mCash, Swich, MobilePay, Apple Pay, Alibaba Pay, PayPal, Google Pay etc. are all nice and temptingly easy to use, but much more expensive, and require several types of point of sale (POS) terminals in each shop. Banks have, of course, tried to attract young customers with fun and easy solutions on the mobile, while at the same time creating problems for others.

As the most widely used payment app in Norway, Vipps does not communicate with POS terminals in shops. Apple Pay has secured the right to control the use of NFC signals for all iPhone users. This means that if you have an iPhone, you cannot use MCash or Mobile Pay. Instead, you may be forced to use Apple Pay in large chain stores such as Rema and Narvesen, and many other places with NFC payment terminals. Today, MCash and MobilePay only work with a QR code even though 85% of all POS terminals in Norway have modern communication with NFC. Apple Pay can become the one and only choice for everyone with an iPhone – and that applies to a large group of people.

This chaotic situation, described online by Finance Norway and BITS, has scared Norway's major retailers into forming their own company; Retail Payment, working to develop a common solution for communication with the many wireless POS payment solutions which will soon be flooding the market.

There is a crying need for a common standard, e.g. a biological footprint that everyone can relate to. The solution may be a PCU, a Personal Secure Cyber-Biological Universal Identification reader, which generates a Cyber-Biological Identity, a CB-ID. The CB-ID replaces your real biological identity, and at the same time, the PCU reader protects your real biological data from permanent loss. By standardizing on a PCU CB-ID solution, the banks will be able to coordinate their own systems with NFC payment on most existing POS terminals. And if the payments are routed via local payment partners such as BankAxept and NETS, great savings can be made.

This is important to avoid a situation where the banks and traders eventually will have to shift today's high level of costs onto the customers. Mobile payment is so far free of charge to the customer, leaving the banks to pay the bill from foreign payment partners such as Visa and MasterCard. The PCU solution can simplify and secure payments for everyone, while at the same time protecting real biological data from hackers and criminals. With a Personal Secure CB-ID, both banks and public authorities can settle on one common standard for both payment and common registration in their databases.

Putting the person first by securing the users' biological data is the only way forward for both banks and national database solutions. Everything connected online is exposed to risk, and everyone in need of safe digital identification should use a PCU type solution. Only companies who focus on individual personal safety, offering a free selection of services, will succeed in spreading their solutions to a wide audience.

[Translated from article published I Kapital 19/2016]

Fulfil ancient dream for the future:

Roadmap for the future, the Norwegian house, moon landing and not least, it is typically Norwegian to be good!

Isn't it typical norwegian to be best?

Norwegian solutions as PCU is invented and patented to ensure an important development to prevent the digital nightmare we can all be part of if all our biological data are stolen.

From seven years of research and development it has emerged an ideal personal safe biologic identification of a person safe enough for a "National ID" and "Bank ID" without putting the real biologic values at risk

A national dream come true?

- PCU create the ideal person secured «Biologic National-Bank identification», "CB-ID".
- CB-ID is the person secure and exact biological ID to be used in a National Reference.
- PCU registration and identification should be supported by Parliament, BITS and Inspectorate.

CB-ID?

What is a PCU and CB-ID?

PCU will provide the necessary personal safety for biologic identification from face, fingerprint, iris and voice. PCU generates a cyber biologic ID, called CB-ID, which ensures that only the right person have access to payment, banking, access and other services, while the person's real biological data is secured. CB ID created by a mechanical and manufacturing technical solution, which create a biometric simular ID but with entirely different values than the real biological values. The generated CB-ID is then encrypted and sent wirelessly to the receiver. Even under the communication the CB-ID can be doble encrypted by a free variable selection to makes it impossible to use if stolen.

Read more on www.pcucompany.com

PCU can easily be interoperated with existing solutions if desired (Bypass ID Commfides email ID, Nemi ID DK, Bank ID SE, Telia e-legitimation, Tupas (Finland), Bank ID, Passport, bank, VISA, MasterCard or Amex and national ID card)

PCU Company has an objective to first provide products and a safety solutions to the major service providers throughout Norway / Scandinavia and futher on if they (the Scandinavien providers) do not expand rapidly seling the joint solutions throughout EU / US /world.

PCU units are based on the future mobile technology giving the PCU the most incredible opportunities. The patented PCU innovations can advantageously be implemented wherever there is a need for accurate authentication.

PCU can be a small separate device that fits in your wallet, on a jewlery or implemented in a wristwatch or a mobile and as part of an ornamental or medical “wearables”. About 10 to 15 years from now the PCU with nanometer manufacturing technics can integrate DNA readers for identification if desired or be produced so small that it can be integrated into the body, “PCU as Insideables.” Then the PCU implants stolen from famous / rich people when doped down and remooved will not work without reading their biologic CB-ID, as the current code implants today.

PUT THE NORWEGIAN HOUSE IN ORDER.

How much is a PCU simplified future worth for Norway?

There can be many large financial savings over years if everyone can confirm its exact biological identification, CB ID without meeting up with passport, bank cards, national ID cards and the like, in order to authorize small or large activities or transactions as buying a house, buying medication or vote in premises that have been discontinued.

PCU makes all type of banking, trade and large payment service through actors as Nets, Klarna, Visa and MasterCard safe. Norwegian industry using PCU can easy developed solutions that averts the current nightmares and create a future with an exact personal safe National-Bank ID, CB ID.

NATIONAL ROADMAP FOR THE FUTURE.

How important is a PCU secure and simplified future for Norway?

Vast opportunities for efficiency may be the future when everyone is registered and can be identified over the Internet with their secure, unique national CB-ID without having to use passport, BankID, creditcard or equivalent.

Universal standard with unique, universal, person secure and person CB-ID readout will quickly provide major savings and simplification for all, as in healthcare, NAV, Tax Administration, Housing Bank, Immigration, school, military, police and may be the only choice for thous with biologic handicap.

Norwegian solution industry can indeed conquer EU with PCU CB-ID solutions support in Edias (e ID in EU). When state and local authorities have approved “CB-ID” for person secure identification in Norway the same has also to be accepted throughout the EU.

Creating exact and person ensure national CB-ID / Bank CB-ID may soon become a wish that goes far beyond Europe. It will create many new jobs in a Norwegian international security industry with PCU origins and solutions from Norway.

A close cooperation with the necessary support from KMD-DIFI required to create a new

Norwegian and safe reader for National CB-ID suitable for general use in a National ID base, to everyone's benefit.

DIGITAL "moon landing"

Rethinking personal identification with their mobile number and PCU with their national «CB-ID» where mobile phone number follows us throughout our lives, just as license plates follow the car to the scrapped. Young people are registered with Social Security number in the national base until one is big enough to use their own smart mobile and PCU.

Everyone presents themselves with their mobile phone number and verify / identify themselves with their secure CB-ID from the PCU as National ID or Bank ID. This will create additional security and not at least simplicity the lives for young and modern citizens living online through their mobile, for every thing.

Such a "digital moon landing" will ensure mobile use for everything at home, in the car, secure payment at trade, shopping, travel, entertainment, internet banking and online payments.

We have many government innovation actors, as Research Council, Innovation Norway, Kavli fund Norforsk, Euro stars, H2020 and OFU / IFU. They all should contribute to help Norwegian industry conquer EU with innovative PCU type CB-ID security solutions under Edias (e ID in EU) as soon as they have deliver PCU solutions to the state and municipality. PCU, CB-ID as "National ID, CB ID" for person secure identity in Norway have the same acceptance throughout the EU.

PCU Company looks forward to close cooperation with Norwegian industry, government and big banks for common PCU development. PCU should be accepted by Banks, BenkID, BITS, credit card companies and KMD / DIFI to create the person secure national ID and national ID -base that everyone wants, to everyone's benefit.

Additional major advantages for Norwegian banks.

The Norwegian banks will soon be able to be a few years ahead of its competitors abroad includ f Sweden and the rest of the western world in entrepreneurship in retail payments.

By leading the development, vinning the mobile payment market with new Vipps and Mcash will create banks' expansion outside Scandinavia. The Norwegian / Scandinavian banks can then prepare campaigns to recapture domestic markets and not least enter into separate and early appointments with new and old payment processors Nets, Bank Acceptance, Visa, Klarna, MasterCard, AMX, AliPay, PayPal, GooglePay etc.

Then we are good and may win the future with our new roadmap for moon landing of the Norwegian house.

Securing it all

The PCU

A Personal Cyber-Biological Universal ID Unit for generating CB-ID's

Is it for me?

The PCU is for everyone using mobiles or smart keys for access, payment connections, banking and operation of all digitally controlled solutions.

What does it do?

The PCU generates a Cyber Biologic ID (CB-ID); A personal safe, unique and accurate method of identification without jeopardizing your real biological data.

What makes it so special?

Your personal Biological ID is secure using a PCU! Your biological data cannot be stolen, as you are identified by the PCU generating a CB-ID, a unique, replaceable Cyber Biological ID. As the CB-ID is unlike your real biological values, your real biological data are not stored in the unit, or any other place.

How do I change my systems to use PCU?

No change is needed! The PCU generates a wireless ID signal in the same way as most types of standard biometric ID solutions. The PCU is merely an addition to enhance the biometric readings you use, bringing high personal security to the user. If one or more of your service providers do not offer the PCU solution, you should ask them to adapt their services to become a future partner with PCU safety.

Make your life simpler and more secure:

Ask for a PCU solution from your service providers today!

PCUCompany.com

PCUCompany.com

PCU Company

Idrettsveien 10
1400 Ski - Norway

info@pcu.no

facebook.com/pcucomp
twitter.com/pcusec
linkedin.com/company/pcu-company