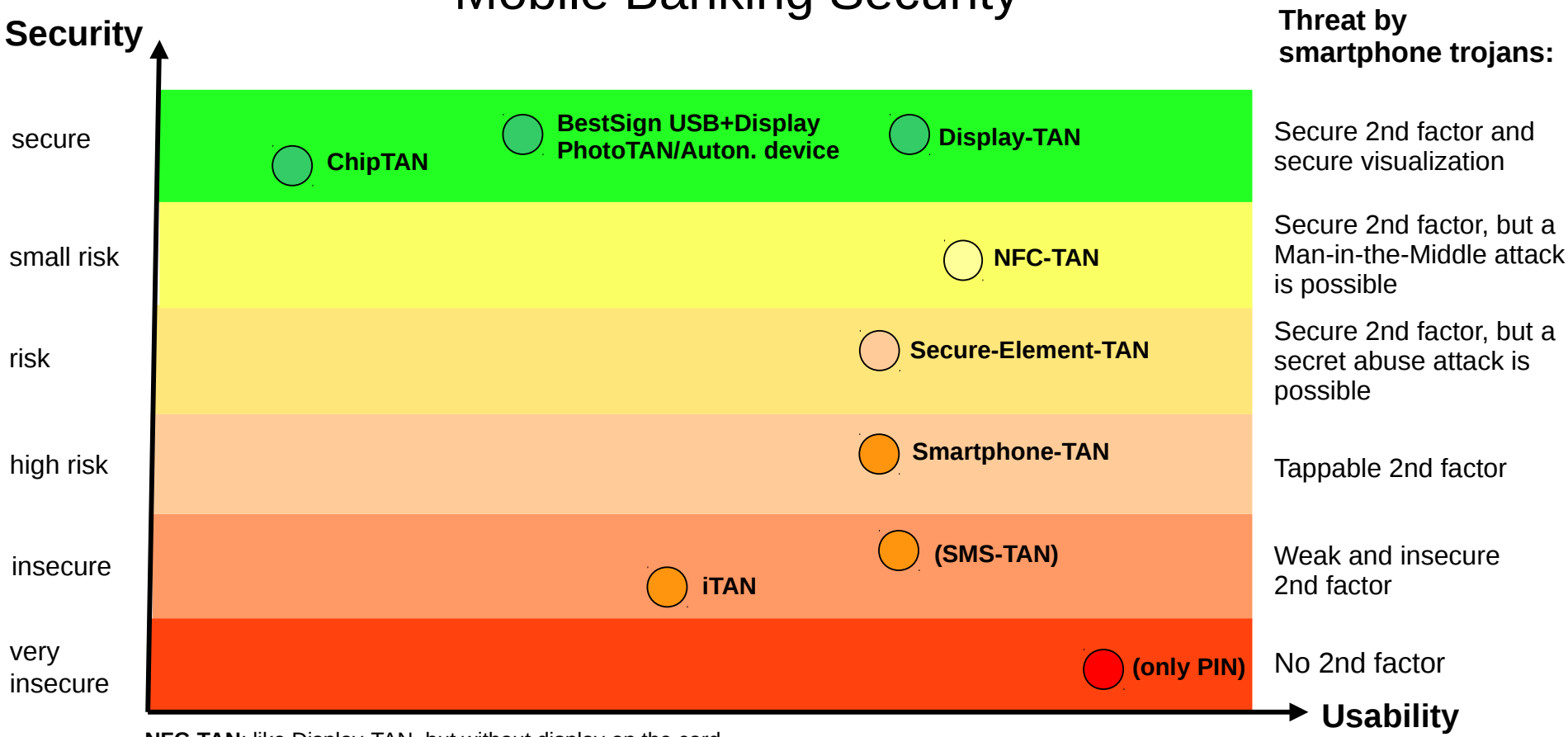
Mobile Banking Security



NFC-TAN: like Display-TAN, but without display on the card
Smartphone-TAN: Bank credential is stored on the smartphone. Examples: PushTAN, Photo-TAN/App, BestSignMobil
Secure-Element-TAN: like Smartphone-TAN but with credential stored and processed on a Secure Element, like SIM card or hardware Keychain. Example: If an iOS banking app uses the iPhone KeyChain this iOS App could be called a Secure-Element-TAN.

- The security evaluations mainly refer to the danger of smartphone malware.
- Smartphone malware includes „fake apps“ which are fraudulent smartphone apps which look like the bank app and which are planted on the bank customers. In fact, fake apps may be the most dangerous threat because they can easely be written.
- All listed methods use a second factor what-you-know which is insecure, i.e. tappable by smartphone trojans.
- The methods set into parentheses (...) are in Germany not used for Mobile Banking - because of security reasons.
- Even on the methods evaluated as secure there are potential attacks: „Social Engineering“, or Man-in-the-Middle attacks which expect unattentiveness of the bank customer. Nevertheless, with these methods - and only with these - the bank can be sure in a case of fraud that the customer has made a grossly negligent mistake, and can refuse to compensate the damage.

B. Borchert, June 2015, www.display-tan.com