File encryption

You work for a mobile device manufacturer and you have been asked to chose a type of device encryption for your next Android smartphone. You can chose between full-disk encryption (FDE) and file based encryption (FBE). Now, consider the following scenarios

Market research has shown that users are interested in "transparent operation mode“

1. What does "transparent operation mode" mean?
2. What are the security guarantees that you can offer to users which activate the "transparent operation mode"?
3. Which of the two systems (FDE and FBE) is better if you want "transparent operation mode"? Explain your answer.

File encryption

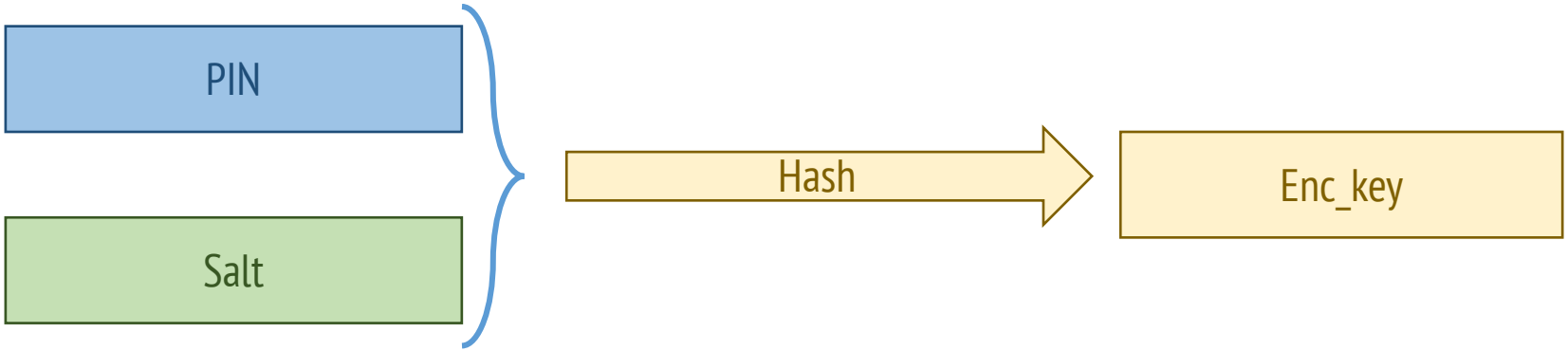
You work for a mobile device manufacturer and you have been asked to chose a type of device encryption for your next Android smartphone. You can chose between full-disk encryption (FDE) and file based encryption (FBE). Now, consider the following scenarios

You want to speed up the boot process of your device by encrypting less data.

1. Which of the two systems (FDE and FBE) will you chose and why?
2. Give one additional positive feature gained from you choice.
3. Give a potential negative effect gained from your choice.

File encryption

Consider the key derivation scheme in the figure below, where "PIN" is a 4 digit pin and "salt" is a public random value.



1. Which is the entity being authenticated ?
2. What is the role of the salt?
3. What is the purpose of the hash function?
4. Are there any attacks possible against this scheme? Explain your attack and a possible fix for it.

File encryption

What are the security implications of using a public, hardcoded and known value for the “default password” in Android 5.0?

How does it compare to not using encryption at all?

Explain your answers by referring to security aspects (confidentiality, authentication…), and difficulty of use.