Cartão independente

BIOMETRIA **Eduardo Correia, investigador do INESC TEC: «O CC deixa de usar um software que é uma caixa negra e passa a ter acesso ao código-fonte da solução que faz»**
Fotos: Lucília Monteiro

Com o desenvolvimento do software que gere impressões digitais no Cartão do Cidadão, a Imprensa Nacional – Casa da Moeda acabou com a dependência de um único fornecedor

Hugo Séneca

Com uma memória RAM que na melhor das hipóteses terá 8 KB e a capacidade de envio de pacotes de dados de 256 Bytes, o chip do Cartão do Cidadão (CC) dificilmente poderá ser considerado um portento computacional. E no entanto cada um destes chips suporta uma das funções mais críticas na organização do Estado: confirmar que as impressões digitais dos dois dedos indicadores de cada português são realmente aquelas que são apresentadas sempre que é solicitada a identificação. Até ao início deste ano, a comprovação de impressões digitais era

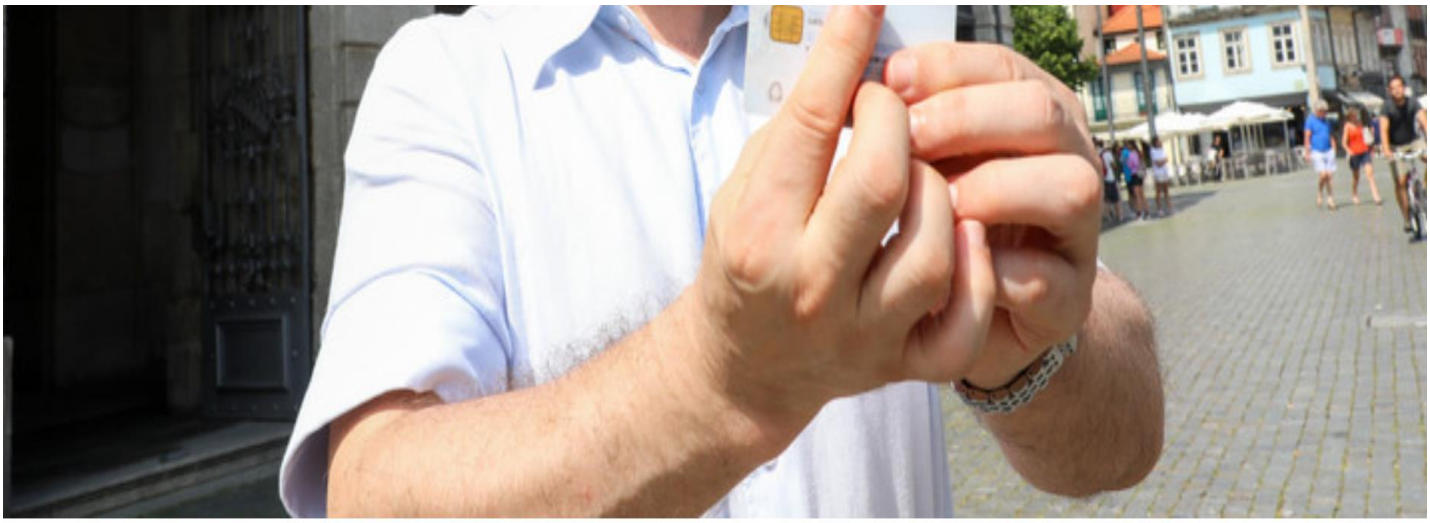
feita com software comercial fornecido pela Gemalto, que fabrica os chips do Cartão do Cidadão, mas de ora em diante, os títulos de identidade nacionais passam a usar tecnologia made in Portugal: O INESC TEC desenvolveu a pedido da Imprensa Nacional – Casa da Moeda (INCM) o software que, num único segundo, permite fazer o "match" entre as principais referências da epiderme dos indicadores e a informação que se encontra armazenada no cartão.

«Esta evolução representa um acréscimo de segurança. O CC deixa de usar um software que é uma caixa negra e o Estado passa a ter acesso ao código-fonte da solução que faz o "match" das impressões digitais e, por isso, sabe como tudo funciona», explica Eduardo Correia, investigador do INESC TEC e professor na Faculdade de Ciências da Universidade do Porto (FCUP).

Além do controlo total na tecnologia usada, o desenvolvimento do software que faz o "match" entre impressões digitais tem vantagens do ponto de vista financeiro e comercial: «A solução anterior era muito cara para o Estado. Se tivermos em conta esses custos, verificamos que, em apenas alguns meses, a ferramenta que desenvolvemos fica paga», sublinha Eduardo Correia, lembrando de seguida outra virtude da substituição do software que faz o "match" de impressões digitais: «Mas ainda mais importante do que o que se poupa com o licenciamento é a capacidade que o Estado ganha para ir ao mercado e poder escolher entre vários fornecedores de cartões do cidadão que podem concorrer entre si».

Minúcias dérmicas

Há dois anos que a INCM e o INESC TEC começaram a trabalhar para criar a última peça que faltava para o Estado ganhar a independência face à Gemalto. O projeto tinha dois desafios técnico de maior complexidade: 1) a Constituição Portuguesa proíbe o tratamento massivo de dados biométricos dos utilizadores e, por isso, os dados não podem ser extraídos do chip do cartão; e 2) a solução que viesse a ser criada teria de garantir que os dados são comprovados em menos de três segundos, como determina o standard internacional, e desejavelmente em menos de um segundo, como a solução anterior.



FALHAS **Eduardo Correia recorda: «esta solução respeita o standard da identificação biométrica internacional, que prevê a ocorrência de um falso positivo em 10 mil casos»**

Passados os dois anos de desenvolvimento, o INESC TEC pode reclamar os louros do trabalho: o software desenvolvido para a INCM está apto a confrontar as denominadas minúcias (pontos de referência) que tenham sido obtidas através de um leitor de impressões digitais e confrontar esses dados com a informação que se encontra armazenada no chip em apenas um segundo. Como determina a lei, os dados biométricos nunca saem do chip – e o "match" é verificado dentro do cartão.

Antes de começar a ser distribuído com os CC, o software teve de passar pelos testes do Instituto Nacional de Standards e Tecnologia (NIST) dos EUA. «Vai sempre haver falsos positivos, mas sabemos que esta solução respeita o standard da identificação biométrica internacional, que prevê a ocorrência de um falso positivo em 10 mil casos. Também neste caso a solução do INESC TEC é comparável à solução da Gemalto», conclui Eduardo Correia.

MAIS ENCRIPTAÇÃO

A nova solução de "match" de impressões digitais do Cartão do Cidadão (CC) foi desenvolvida para ser compatível com a tecnologia Java Card. Além da biometria relacionada com a gestão de impressões digitais, o pequeno chip do CC corre ainda um segundo módulo que armazena a assinatura do titular (conhecido pela sigla IAS). A Imprensa Nacional - Casa da Moeda (INCM) informa que não há qualquer plano para desenvolver uma versão própria do módulo IAS: «A tecnologia que usamos tem todas as garantias de segurança. Além disso, há cinco fornecedores desta tecnologia e não estamos dependentes de um único», explica Gil Rodrigues, diretor Comercial e de Marketing da INCM. A evolução tecnológica do CC vai prosseguir mantendo a segurança como um dos principais vetores: em breve, a INCM vai começar a distribuir CC que, em vez da encriptação de 2048 bits, já deverá contar com uma encriptação de 3058 bits. «É uma questão de segurança informática. Com a evolução da computação, pode haver alguém que tente vencer os códigos do CC. Com o novo sistema de criptografia, estamos a antecipar-nos com o objetivo de tornar mais difícil o trabalho de quem queira decifrar os dados que estão no CC. E isso é feito com um aumento do poder de computação do chip do CC», acrescenta Gil Rodrigues.