ABECS 3DS NORMATIVE – Review of proposal

Peter Bayley
peter.bayley@merchantriskcouncil.org

1. The MRC

The Merchant Risk Council (MRC), a global non-profit membership association founded in 2000 that represents professionals in payments and payment fraud prevention.

The MRC organization comprises over 750 members – including merchants, banks, PSPs/acquirers, solution providers and law enforcement agencies – spanning North America, Europe, Latin America, and Asia.

Approximately 66% of MRC members are merchants, and we are committed to working collaboratively with payments industry stakeholders to ensure the merchant perspective remains central in discussions surrounding the continuous evolution of payments.

2. Introduction

ABECS is described as the Brazilian Association for Credit Cards and Services Companies who are positioned as responsible for creating self-regulating mechanisms and establishing the best practices for companies in Brazil for the payments sector.

The organization brings together card issuers, acquirers, banks and card schemes to discuss and agree technical and commercial standards. It should be noted some major merchants are included in some debate, but merchants don't appear to be listed as members[1]

Although not a government regulatory body ABECS members are expected to adhere to its rules and standards, which effectively become the default standard for card companies in Brazil.

There are understood to be circumstances in the past, where Brazilian regulators have formally adopted standards, and in this circumstance formal regulatory powers / enforcement become effective.

It is worth noting that Brazil does not support cross border acquiring, and if it did so the complexity of the Brazilian payment arrangements (installment support, complex value dating solutions et al;) would require a high level of customization. As such, in addition to domestic merchants, any international merchant operating in Brazil via a local acquirer will be subject to ABECS requirements.

In this light, on 21 August 2024 ABECS issued a document broadly entitled (when translated from Portuguese) as "Normative 031 regarding technical standardization for the application of authentication via Version 2,0 or higher of EMV 3DS based on minimum values by ecommerce groupings." – See Appendix 1 for the ABECS paper link and an English translation.

[1] https://abecs-org-br.translate.goog/empresas-associadas?_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp&_x_tr_hist=true

This ABECS document calls for the use of 3DS by merchants, issuers and acquirers 180 days after the paper has been published (17 Feb 2025).

This MRC paper seeks to summarize the ABECS paper and the potential implications for MRC merchants impacted by this ABECS proposal.

3. Brazil 3DS context

Brazil is a historic high inflation market, with a payment system uniquely adapted to such an environment, such as its tradition of payments via installments, value dated settlement pricing and similar.

Card payments are traditionally high cost by international standards and have also tended to experience significant friction with high decline rates.

In recent years, card payments have been significantly impacted domestically via the Pix payment network which utilizes internet bank payments initiated by a mobile phone app (most typically, the customers own banking application – although third party versions are now evolving).

Pix has been strongly advocated by the Brazilian regulator, who continues to seek reform and enhancement to Brazilian payments. Pix implementation benefited from significant industry discussion and contribution during its creation and improvement, which has resulted in significant success and massive growth as a payment solution.

3DS capability by issuers in Brazil is believed to be reasonably strong, although far from universal. The 4th largest card issuer is believed not to support 3DS2 at all at this stage.

Merchant deployment is understood to be comparatively limited. Whilst numbers have not been easy to determine, it is believed that less than 40% of merchants currently support 3DS

Risk based authentication (sometimes referred to as silent or passive 3DS authentication) is understood to be utilized by issuers, but again statistics on performance do not appear to be readily available, and anecdotally the usage is not optimal.

Merchants are very concerned that the ABECS' 3DS proposal is not well defined and has not benefited from review and validation. They are therefore concerned that any implementation via the current proposed model may have serious practical and commercial implications leading to failed transactions, lost sales and significant degradation of customer experience.

Some merchants have reported recent cases of instability of one credit card network that caused significant impact and lost sales. Stability of the current infrastructure is therefore a significant concern.

Whilst further statistics are being sought, anecdotal merchant experience is detailed within this paper and some formal statistics are set out at Appendix 2.

4. ABECS High Level 3DS requirements

The ABECS document is published in Portuguese and therefore this summary has been prepared from a translation of the document and in close collaboration with the MRC office in Brazil.

However, please note that this may result in some miss-translation and positioning of the paper's proposals, and readers are urged to consult with the full paper linked at Appendix 1 of this document.

4.1. Over-riding approach: All merchants offering remote payments via a Brazilian licenses acquirer/PSP for Brazilian credit, debit or prepaid issued cards, will need to support EMV 3DS2.0 or higher.

4.2. Remote payments (ecommerce transactions): will, effective 17 Feb 2025, be required to undertake 3DS authentication where:

- The card is not an anonymous prepaid card
- The card is not a corporate card (except for self-employed professionals who work independently). *It is assumed that these can be clearly defined in Brazilian payments, but this definition sounds unusual so may reflect a poor translation*.
- The merchant is not listed on a compliance program and transactions are for a value above the limit set for that merchant MCC (values are listed by MCC in the ABECS paper – but are typically between US$10 – US$180)

4.3. Exemptions: Article 6 states exemptions may be agreed for 3DS subject to evaluation and ratification by the ABECS Fraud Prevention and Security Forum. This includes:

- Recurring transactions
- On File (assuming to mean card on file) transactions
- Typed transactions (assumed to mean Mail/Telephone Order transactions)
- Exception lists defined between issuers and merchants (e.g. eligible for the pinless online debit program)
- Other transactions not otherwise specified where the cardholder is not present at the time of the transaction

It is hard to entirely understand what these exemptions mean in practice, what each exemption exactly covers, whether they need to be agreed by the committee for each merchant, or will be agreed generically et al.

4.4. Issuer 3DS adoption: Article 10 requires that issuers must ensure that authentications see a minimum approval of:

- In 2024: 85%
- In 2025: 90%

It is unclear whether this is talking to approval rates or successful authentications.
Non active BINS (again undefined) must not see more than 3% of authentications.

4.5. Issuer Risk-Based Authentication: Issuers are expected to respond to 3DS authentication requests in line with agreed scheme SLAs and to support Silent authentication (Risk Based Authentications/Passive authentication) based on the device used.

In addition, issuer Risk Based Authentications (RBA) must be a minimum of:

- In 2024: 30% (although this proposal doesn't apply until 2025)
- In 2025: 40%

4.6. Merchant Data Sharing: Merchants are required to share all mandatory data with issuers. *This is assumed to be the data already required by international card schemes but may be defined differently.*

4.7. Sanctions for non-compliance: For non-compliance the normative seeks a referral to the Security and Fraud Prevention forum which can then further refer to the IAP, Payment Arrangement Institutions, companies that are appointed by the Central Bank (Bacen) through its regulations. *There appears however, to be no clear sanction for any party's failure to meet the requirements set out in this normative*

4.8. Timeline: The ABECS document advises that "This regulation comes into force from its date of publication with effective implementation 180 days after publication." This implies that the expectation is that all parties are fully compliant with the requirements set out in this paper by 17 Feb 2025.

However, whether the intention is that work starts to deploy the infrastructure at this time, or whether 100% deployment is expected to have been achieved by this date, is not entirely clear.

5. Potential Areas of concern

The remainder of this paper looks at potential areas of member concern, with each section setting out the high-level issue and comments re impact and potential positioning.

5.1. Statistics on current environment (issuer readiness, merchant deployment, auth rates, RBA support et al)

In summary:
The ABECS proposition tends to be light on metrics, with minimal data on current performance and no projections in terms of impact during implementation or expected outcomes once implementation of the proposals are deployed. This makes it difficult to assess the extent to which the market is ready for the proposed implementation, the impacts of deployment and the costs to deploy together with the proposed benefits that will be achieved.
.

Implications:
The ABECS proposal does not quote the metrics used to determine the actions proposed nor the benefits that the approach is expected to realize.

In particular:

- **Fraud and Chargeback assessments**
  The normative provides no detail on the expected fraud and chargeback savings that may be anticipated from deployment, nor the expected costs to achieve such. A proposal with no vision of expected costs and benefits is a concern. How will success be measured, failures be identified and swiftly addressed if a plan and success criteria is not articulated?

- **Issuer readiness does not appear robust.**
  Merchants advise that they currently see issuers fail to approve 3DS authentications more than 50% of the time. This indicates issuers' performance falls far short of the levels indicated in the ABECS proposition and is not yet viable to support the ABECS proposal as stated. A 50% failure rate would significantly disrupt card payments.

  Poor implementation of 3DS has been proven to create a 50% or higher decline rate in authentications in some other countries (see Riskified report[2]) and Brazil needs to ensure that these lessons are learnt.

  It is essential that issuer performance is formally reviewed and confirmed robust prior to the mandatory deployment of SCA. If these validations have occurred the performance assessments and metrics should be shared

- **Risk Based Authentication (see 4.3)**
  Silent or Risk Based Authentication (RBA) appears to be used comparatively infrequently in Brazil and the plans for roll-out (of 40% by 2025) indicates that issuers in Brazil are not well positioned to support this. It would be useful to understand the expected volumes (given these are presumably minimal by issuer)

- **Fraud targets and appetite**
  Brazilian merchants advise that the current chargeback rate runs between 0.8% to 1% with card scheme published excess rates set at 1.5%-2%, (dependent on Card Scheme). Whilst these rates are high compared to many cross-border markets, Brazil has particular legacy infrastructure and risks which drives higher risk. Given the card scheme published risk appetite in Brazil the rationale for mandatory adoption of 3DS authentication via ABECS self-regulation at this time is unclear. As mentioned above, what is the proposed optimal fraud target here?

[2] https://www.riskified.com/blog/what-merchants-should-know-when-considering-3d-secure-2-0/

- **Impacts on pricing**
  Given that fraud and fraud management traditionally reflect a significant proportion of the interchange fee costs, presumably it is anticipated that interchange fees will reduce as fraud reductions occur. Merchants may be able to take comfort if the intent, values and timing here could be articulated.

- **3DS Floor Limits**
  There appears to be no justification detailed for the floor limit model by MCC above which the normative proposes that 3DS authentication must always be sought by merchants.

  Given the costs of deployment and the balance of cost v benefit that is required to ensure sensible deployment, it would be useful if the detailed model and calculations used to derive these values were shared.

  In addition, during dialogue with the MRC merchants have argued that instead of using the MCC 3DS floor limit values, which by default will consolidate merchant performance, that fraud and chargeback targets by other vectors such as by merchant or acquirer could offer a better approach.

  Merchants remain concerned that by only utilizing 3DS floor limits by MCC without considering average transaction values, fraud and/or chargeback levels may result in ABECS inappropriately focusing 3DS towards environments where problems do not exist.

Proposed Merchant/MRC positioning:
It is proposed that ABECS update their document to include the detailed metrics and positioning to better define their proposition and approach.

This can then be shared with all stakeholders (including merchants) with a view to determining and validating:

- an optimal approach for Strong Customer Authentication (SCA) deployment
- the current status of issuers' readiness and that this is reflected in deployment plans
- an appropriately phased implementation.
- clear metrics to be tracked prior to, during (see 4.6) and after deployment to ensure payment performance remains stable, reliable and operating effectively
- how the reduced costs achieved from fraud reduction will be sensibly shared between payment stakeholders

5.2. Merchant Consultation and Engagement is critical for successful implementation

In summary:

Merchants have not been properly engaged in this process, and in fact the entire discussion appears to have been limited to ABECS members. The normative paper appears to be the first time it has been shared externally. As such, it is light on detail in areas that are important to merchants and regarding some practical elements of implementation.

Implications:
The ABECS normative proposition has not been subject to review by the wide cross section of merchants that will be impacted by the proposal. In practice, it is not clear that it has been publicly reviewed and debated outside of the ABECS immediate community.

This means that the normative has not been subject to robust review, with the risk that assumptions have been made and full implications not understood.

In particular:

- **No public review**
  Merchants note that the public hearings held by ABECS were limited to ABECS members only, and those merchants do not represent the whole market and were not elected by the industry to lead on such important changes.

  Merchant have suggested to the MRC that ABECS should replicate the process used by Central Bank of Brazil (BACEN) when implementing PIX, which diligently worked alongside merchants to define PIX guidelines and application, with a phased and gradual approach and transparency along all the way.

- **No assessment of cost or inflationary drivers**
  Merchants advise that implementing the normative as currently defined will bring dramatic economic impact and inflationary pressure, which the proposal has failed to recognize or quantify. The impact on merchant costs, and the extent to which the mandatory implementation of 3DS technology will result in additional cost being passed on to consumers, should be assessed as part of an impact statement.

- **Learning lessons from other country implementations**
  Merchants believe Brazil should assess the international evaluation, adoption and use of 3DS authentication.

  A European Commission study published in 2023 to evaluate PSD2 policies concluded that in order to achieve a €0.9billion fraud reduction, direct costs of c €5 billion were incurred and transaction failure estimates of up to €33.5 billion.[3]

[3] European Commission: Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Bosch Chen, I., Fina, D., Hausemer, P., Henžel, A. et al., A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2), Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2874/996945

This was incurred with significant industry collaboration, assessment and validation including a wide-ranging public consultation.

As such, if Brazil does not appropriately engage and assess with wider industry stakeholders, including merchants, the impact and outcome could be significantly worse.

- **Exemptions**
  Please note the section of exemptions below (5.3), which is also noted here as a major area where stakeholder collaboration, is essential.

- **Unbalanced costs and benefits**
  Merchant costs are not appropriately recognized or assessed in the normative, presumably because of the limited merchant engagement during this process.

  Merchants that adopt 3DS are required to implement significant technical changes to their sales IT and infrastructure, enter into new vendor agreements to facilitate the 3DS merchant plug-in, adjust their sales process to collect, collate and make data available to issuers via the 3DS message flow and manage the exceptions driven by an increase in:

  (i) authorization declines
  (ii) abandonment due to friction
  (iii) 3DS failure
  (iv) increased time required by users to pay

  In addition, merchants also face technical errors due to the multiple authentication and authorization steps 3DS requires. All these factors lower overall conversions, harming revenue generation and profitability/cost which will have to be passed, in part or full, to consumers.

  Meanwhile, the issuer benefits from additional data to make detection decisions, an additional opportunity to deny or further validate cardholder instructions and (hopefully) reduced fraud and dispute rates.

  Whilst as already mentioned, these should in time be reflected in interchange fees (although the normative remains silent on this option). Providing merchant incentives earlier would significantly ease implementation costs and drive more effective adoption.

Proposed Merchant/MRC positioning:
MRC would ask that the entire normative document be formally issued for public consultation and updated to allow merchants and other stakeholders to highlight opportunities to better balance the proposition.

For the avoidance of doubt, merchants are supportive of appropriately enhanced payment security – it is in their interest as much as the other payment stakeholders for payments to be efficient and trusted. However, the failure to consult whilst no doubt an oversight, is one that has significant implementation, resilience, cost and economic impacts.

By working with stakeholders to develop a holistic approach, the major problems may be avoided and a more effective solution deployed, delivering a more effective outcome and removing a number of potentially expensive risks.

5.3. Exemptions are unclear and No Risk Based Exemptions

In summary:
Whilst the normative does assume that exceptions will be allowed, these are based on referral to an ABECS committee, and it looks as though the intent is to have them reviewed/approved on an ad hoc basis.

This means that the exemptions will be defined over time and will lead to inefficient implementation as the basis for deployment will change as different acquirers/merchants seek to support different exemption models.

This will lead to inconsistent merchant and customer experience, as well as making exemptions a competitive rather than a collaborative issue.

In summary, the approach is poorly defined and will lead to delays, increased implementation costs and an unbalanced competitive environment.

Implications:
The criteria provided in the 031/2024 normative for exceptions is unclear:

- **Willingness for exceptions, but little clarity on what these are or how they will work**
  Whilst the text indicates a willingness for exceptions, this does not appear to have been given adequate consideration and (as mentioned before) has not been discussed with merchants impacted.

  For example, card-on-file transactions, online debit programs, or recurring transactions, prepayment models et al are listed, but operating approach is not defined.

- **Inefficiency and unbalanced competitive market**
  Exceptions appear to be subject to referral and approval by an ABECS committee, but whether these will work at industry, MCC or merchant level; is unclear.

  A lack of clarity on exemptions will inevitably delay implementations where variants are sought from the committee and could even make (given the anticipated issuer performance on 3DS) exemptions a competitive issue between merchants, inevitably delaying implementation as work is paused as exemption approaches are considered.

This also means that as exemptions are granted, merchants will reverse engineer exemptions not previously anticipated into their 3DS platforms – undoubtedly creating sub optimal IT platforms and solutions.

- **Transaction Risk Analysis (TRA)**
  As previously discussed, many merchants in Brazil qualify for and operate under a "Transaction Risk Analysis" SCA exemption to PSD2 when operating in Europe. This approach has been reviewed and will be retained in PSD3 as a sensible model.

  Given the EU costs and issues with 3DS deployment, and their ongoing support of TRA, Brazil should seek to learn the European lessons and include this flexibility in the Brazilian normative proposals.

Proposed Merchant/MRC positioning:

A failure to adequately define exception models whilst simultaneously proposing short timelines for implementation, will only lead to confusion, potentially unbalance the competitive playing field and drive further costs/implementation issues.

It is strongly recommended that the lessons from other country implementations are learnt, and exemptions properly defined prior to any implementation progressing.

5.4. ABECS Should not be mandating a single SCA technical solution

In summary:
Whilst a country can conclude that a given level of security requirements are required to minimize fraud or disputes, focusing only upon one single technological solution standard is rarely sensible and often anti-competitive.

Strong Customer Authentication may be supported in various manners. Examples already exist around the world, such as the bilateral agreement between banks (such as via the solutions deployed in France), via technological platforms (such as Google Pay or Apple Pay) or directly by issuers (*on-us* traffic for example was traditionally managed directly between the acquirer and issuer where they were part of the same organization).

Focus should be on the required security outcome/principles rather than the technological approach used to achieve such (for example, the PSD2 requirements in Europe do not mandate 3DS, but do require Strong Customer Authentication – the technological approach to achieving such is not considered an area of appropriate legislative or regulatory control).

Implications:

Core principles, not specific technologies, should be the foundation of market payment

regulations.. A failure to uphold such a position can lead to:

- An unbalanced competitive landscape with certain players obtaining advantage based on their ability to offer products, or control standards;
- A lack of innovation in payment security, which if instead was allowed to flourish would enhance capability and reduce cost;
- Higher costs, as players are restricted to a single technical solution.

Proposed Merchant/MRC positioning:
Any payment security proposal should focus on the core security principles and not the systems or products used to deliver these.

A mandate to require only one approach to deliver security is highly likely to reduce innovation, increase cost and create an anti-competitive environment which in many countries would be considered illegal.

5.5. Mandate enforcement is unclear

In summary:
Any enhancement to the payments ecosystem inevitably creates the need for change by individual players and for these changes to be sized, funded and implementation scheduled. The prioritization process, by default, requires an understanding of the implications of not delivering the change.

In payments, many changes have knock-on effects. If an issuer fails to properly deploy 3DS (for example) then a merchant deployment creates no improved security to the issuer or the merchant, even though the merchant has incurred costs. As such, understanding how any change is to be enforced whether by a regulator, card scheme or ABECS is critical (See also 4.6 below as a related significant factor).

However, ABECS has not set out any enforcement concepts or principles other than the requirement that exceptions be referred to an ABECS committee, which may then be directed, in practice, to the international card schemes (who don't appear to have any clear enforcement rules in place – card scheme responses to questions are awaited).

This approach is unlikely to create clear focus, particularly given how generally the ABECS proposal is defined.

Implications:
A failure to define core enforcement models for mandates risks:

- Low Adoption: Without clear governance and eventual penalties, stakeholders may

ignore the mandate.
- Inconsistent Implementation: Some may comply while others don't, creating fragmentation.
- Weakened Authority: Lack of enforcement erodes trust in governing bodies.
- Competitive Imbalance: Organizations that comply may be disadvantaged compared to those that don't
- Ambiguity: Lack of consequences can lead to confusion about the importance of the change.
- Prolonged Transition: The change may take much longer to implement fully.
- Increased Risk: Non-compliance could result in unmanaged risks across the ecosystem
- It may raise questions as to whether ABECS has the authority or ability to enforce a change of this scale and cost and whether it has Central Bank/Regulator support to the mandate

Proposed Merchant/MRC positioning:
In addition to the collaboration of merchants in defining/reviewing the ABECS normative – which will help lead to a more balanced and fair evolution of the initial proposition – merchants believe that it is fundamental that the implementation of SCA/3DS has clear support of the authorities such as the Brazilian Central Bank (BCB) and Autoridade Nacional de Proteção de Dados (ANPD).

This should allow the approach to be validated, the impacts resulting from the adoption of the principles confirmed as supported and a clear implementation and control infrastructure to track and enforce deployment, defined.

5.6. Monitoring and control of roll-out

In summary:
It is unclear how this proposed complex series of changes will be monitored and communicated to stakeholders.

SCA/3DS deployment as defined is complex, with many moving parts, dependencies and costs, as previously discussed. Yet the proposal offers no clear monitoring, interim targets, or measures to generate reviews and action if business is being damaged or the implementation is stalling.

This approach feels far too laissez-faire given the importance of efficient payments to all stakeholders as well as the success of the Brazilian economy.

Implications:
A failure to deploy appropriate monitoring of a major infrastructure change such as this creates the risk of:

- Implementation Delays: Delays can go unnoticed, leading to missed deadlines.
- Cost Overruns: Without tracking, costs can spiral out of control and benefits missed

- Quality Issues: Defects or poor implementation approaches may not be caught early.
- Failure to Identify Risks: Risks or bottlenecks may surface too late.
- Miscommunication: Stakeholders may misalign on dependencies creating delay, friction and failure
- Unmet Goals: The project may not deliver on intended business needs, or the timeline significantly extended
- Stakeholder Dissatisfaction: Lack of progress reports erodes trust and investment
- Regulatory Risks: Compliance issues might be overlooked, leading to penalties

Proposed Merchant/MRC positioning:
Monitoring, targets and communications on outcomes must be included as a core part of this proposal.

5.7. Timelines for deployment

In summary:
The ABECS normative appears to require full deployment of their 3DS requirements by February 2025.

None of the merchants with whom MRC has discussed this change believe that this timeline is even remotely achievable.

It is noted that this timetable also runs across merchants' busiest sales seasons; Black Friday and Christmas and that many merchants advise they have already frozen their system changes in early September as is normal practice as they approach the busiest parts of the year.

Implications:
Seeking to deliver a major system change such as the generally defined proposal within the ABECS normative, during peak shopping seasons and with the inadequate timing proposed will create the following risks:

- System Outages: Increased demand heightens the risk of downtime and service disruption.
- Operational Overload: Teams may be stretched thin, leading to errors and delays.
- Customer Dissatisfaction: Interruptions or slowdowns could alienate consumers during payment.
- Excess Cost: Fast unplanned deployment will drive cost and inefficiency
- Revenue Loss: Downtime or performance issues can result in significant financial losses.
- Inadequate Testing: Limited time may force shortcuts in testing, leading to post-launch issues.
- Delayed Issue Resolution: Busy season may limit resources available for troubleshooting problems.
- Reputational Damage: Failures during peak times can damage the organization's reputation

- Economic harm: payment disruption could impact sales, inflation and overall economic performance

Proposed Merchant/MRC positioning:
The timelines proposed are clearly inadequate for an infrastructure change of this scale and complexity.

Even proposing this timeline indicates a failure by ABECS to understand the risks, costs and consequences of poor implementation.

In line with the other proposals, this timeline needs to be entirely reconsidered and rescheduled.

6. Overall conclusions

This review by the MRC in close conjunction with its members and non-members, in Brazil and abroad, concludes that the ABECS normative proposal falls significantly short of what is required to evolve payments security in Brazil.

- ABECS is proposing to mandate 3DS rather than a Secure Authentication framework, which will hinder innovation and is probably anti-competitive
- The current environment in terms of 3DS deployment is unclear, with the necessary foundational issuer support looking far from optimal
- There has not been a full industry consultation other than by ABECS members – with merchants in particular feeling they have had no opportunity to raise opportunities or concerns
- Requirements and exemptions are not clearly defined
- Monitoring and enforcement models for the proposed changes are unclear/missing
- The approach does not appear to have formal Central Bank / regulator endorsement
- Proposed timelines for implementation are not viable

As such, deployment on this basis would at a minimum be foolhardy with a real risk of damaging payment reliability, increasing costs (and as a result creating inflationary pressure) and a potential risk to the Brazilian economy from the disruption that payment failures can create.

The MRC and its members are very happy to engage with ABECS to overcome these significant concerns, build out the relationship with the merchant community and help achieve the Central Bank / regulator payments requirements and aspirations.

APPENDIX 1

ABECS Document in full

- Link to ABECS web site: https://api.abecs.org.br/wp-content/uploads/2024/08/Normativo-031-Autenticacao-3D-Secure-21082023.pdf
- Copy of Google translation of paper:

Normative - Authentication 3D S

APPENDIX 2

Relevant statistics on 3DS performance during early implementation from merchants in Europe: Webinar "Microsoft, Amazon, and Google -- The Current State of 3D Secure", Jun 25, 2020.

3DS2.X issuer migration

Issuer 3DS 2.X Adoption *external dependency*	Nov	Dec	Jan	Feb	Mar	Apr	May	May 2020		
								MoM	vs. Goal	Goal
UK	37%	peak dial down	50%	61%	79%	77%	86%	9%	-14%	100%
DE	52%	peak dial down	61%	61%	64%	75%	77%	2%	-23%	100%
FR	12%	peak dial down	37%	41%	66%	66%	84%	18%	-16%	100%
IT	27%	peak dial down	38%	29%	29%	23%	70%	47%	-30%	100%
ES	8%	peak dial down	7%	4%	7%	7%	18%	11%	-82%	100%
NL	22%	peak dial down	17%	37%	41%	33%	63%	30%	-37%	100%
Other	10%	peak dial down	14%	17%	51%	48%	53%	5%	-47%	100%
Total	22%	peak dial down	36%	39%	66%	69%	73%	4%	-27%	100%
Abandonment	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**May 2020**		
								MoM	**vs. Goal**	**Goal**
3DS 1.0	24.0%	peak dial down	30.1%	32.3%	26.3%	52.6%	47.3%	-5%	42%	5.2%
3DS 2.x	8.0%	peak dial down	13.0%	16.7%	10.5%	10.2%	13.6%	3%	8%	5.2%
Total	25.3%	peak dial down	24.2%	24.7%	15.4%	14.7%	14.7%	0%	10%	5.2%
Payments Conversion Rate (PCR)	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**May 2020**		
								MoM	**vs. Goal**	**Goal**
Total weblab PCR	90.3%	peak dial down	91.7%	91.4%	94.20%	94.24%	95.43%	119bps	-262bps	98.05%

Scorecard Results

Data for April, May 2020

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Frictionless Performance					Challenge Performance						Authorization Performance		
Issuer Country	FSR-APP	FSR-BRW	FSIR-APP	FSIR-BRW	CR-APP	CR-BRW	CSR-APP	CSR-BRW	CAR-APP	CAR-BRW	ATA-C-APP	ATA-C-BRW	Δ AR-PS	Δ AR-FAS	Δ AR-CS
Target	> 95%	> 95%	< 10%	< 10%	< 20%	< 20%	> 80%	> 80%	< 10%	< 10%	< 120	< 60	+ 3%	+ 3%	+ 6%
AUT	87.2%	76.1%	42.3%	48.2%	54.8%	59.8%	57.6%	65.2%	32.5%	28.7%	369	64	0.9%	-1.5%	0.8%
BEL	95.3%	94.6%	93.4%	97.7%	22.9%	22.7%	0.0%	53.6%	-	40.3%	-	96	-54.0%	-25.9%	15.1%
BGR	90.9%	95.1%	72.3%	81.2%	12.5%	11.5%	32.0%	67.8%	4.0%	16.9%	39	57	4.0%	-13.5%	9.8%
CYP	96.2%	97.4%	96.1%	97.4%	0.0%	1.0%	-	100.0%	-	#N/A	-	7	5.3%	-5.7%	36.9%
CZE	80.6%	77.6%	68.0%	69.8%	45.8%	44.9%	51.0%	77.5%	20.4%	19.6%	301	47	-16.7%	-3.7%	-27.4%
DEU	86.1%	80.6%	36.2%	55.1%	16.5%	31.5%	14.7%	56.7%	26.9%	29.3%	231	87	0.7%	-10.0%	1.8%
DNK	98.0%	66.9%	79.8%	72.0%	16.8%	90.4%	16.3%	75.9%	49.2%	16.8%	218	53	-4.9%	-4.2%	0.7%
ESP	99.0%	97.6%	97.5%	97.7%	0.0%	0.1%	-	-	-	-	-	216	-33.5%	-20.6%	20.1%
EST	95.6%	93.7%	47.9%	66.2%	0.0%	0.0%	-	-	-	-	-	-	2.3%	-14.6%	#N/A
FIN	97.4%	88.8%	93.2%	87.7%	24.1%	65.0%	26.6%	65.7%	28.3%	22.8%	136	76	-0.3%	-9.7%	0.9%
FRA	94.5%	93.8%	79.8%	81.4%	59.6%	57.6%	42.8%	70.5%	34.7%	24.0%	327	66	-2.8%	-10.4%	6.8%
GBR	97.4%	95.8%	12.7%	16.1%	3.0%	7.6%	70.9%	73.3%	15.7%	14.2%	218	51	-0.2%	0.4%	6.6%
GRC	96.2%	96.5%	68.4%	66.1%	15.8%	9.5%	44.8%	82.5%	24.9%	13.8%	343	33	-6.3%	-4.6%	13.3%
HRV	87.5%	92.6%	80.4%	90.5%	4.5%	7.2%	0.0%	30.0%	-	50.0%	-	159	-7.7%	-14.0%	25.1%
HUN	93.6%	95.6%	60.4%	69.2%	4.5%	10.3%	0.0%	73.3%	-	22.6%	-	91	-11.0%	-0.6%	8.6%
IRL	99.3%	96.5%	30.3%	30.7%	9.2%	14.8%	47.6%	70.0%	43.5%	11.5%	185	65	0.3%	0.2%	6.5%
ISL	90.9%	76.2%	20.2%	10.7%	63.8%	53.1%	54.6%	73.3%	19.7%	19.3%	122	39	6.9%	-34.6%	11.3%
ITA	96.8%	96.2%	83.8%	85.8%	22.9%	26.2%	0.0%	65.6%	-	27.5%	-	60	-4.8%	-12.0%	10.0%
LIE	90.7%	92.6%	34.7%	53.3%	30.8%	8.0%	33.3%	71.4%	62.5%	28.6%	47	37	-63.1%	7.4%	25.3%
LTU	92.1%	97.0%	52.6%	68.0%	0.0%	0.0%	-	-	-	-	-	-	6.4%	-8.8%	#N/A
LUX	99.1%	94.9%	91.9%	88.8%	0.3%	4.4%	-	73.7%	-	10.5%	-	65	19.9%	-31.7%	30.3%
LVA	96.2%	97.0%	52.3%	63.5%	0.0%	0.0%	-	-	-	-	-	-	-4.7%	-10.6%	#N/A
MLT	88.9%	94.8%	22.0%	13.2%	56.8%	44.4%	55.9%	79.4%	13.7%	15.9%	115	29	5.0%	-8.4%	7.1%
NOR	98.5%	77.7%	94.1%	88.2%	22.5%	81.0%	31.8%	69.5%	58.8%	19.7%	345	55	-10.0%	-10.4%	6.6%
POL	97.7%	97.6%	78.3%	82.4%	2.9%	3.5%	41.9%	69.8%	28.1%	16.7%	444	55	3.0%	-2.6%	-1.6%
PRT	98.9%	98.0%	86.8%	93.4%	0.0%	1.0%	-	61.3%	-	38.7%	-	63	6.5%	-15.0%	26.3%
ROU	84.7%	90.7%	89.7%	91.4%	51.0%	51.3%	17.5%	58.5%	31.5%	36.3%	142	47	-1.2%	8.7%	11.0%
SVK	79.5%	92.3%	87.8%	89.5%	11.5%	26.5%	23.9%	77.0%	14.1%	19.3%	170	85	8.9%	-5.3%	8.8%
SVN	51.9%	47.8%	64.3%	87.5%	64.9%	75.7%	2.0%	79.9%	59.0%	15.8%	66	59	-55.1%	-6.8%	14.1%
SWE	94.6%	94.0%	78.2%	84.2%	49.2%	43.2%	52.6%	73.0%	32.7%	14.3%	290	37	-5.8%	-11.8%	8.9%

Observations

- Issuers have yet to enable SCA in some markets
  - CYP, ESP, EST, LTU, LVA, PRT
- Challenge success rates are low to very low
  - Hurts consumers and businesses
- Customers abandon checkout at high rates when challenged
  - Customers are confused and/or experience poor implementations of SCA
- Issuers rely heavily on Mastercard/Visa for authentication stand-in
  - Issuers are not ready with their own implementations
- Authorization approval rates worsen with authentication stand-in
  - Merchants are penalized for lack of issuer readiness
- Authorization approval rates improve when the challenge succeeds
  - Delivering on the promise of SCA

Conclusions

- The ecosystem is not yet ready for SCA
- The ecosystem is unlikely to be ready by 31 December 2020
- Strict enforcement will hurt consumers and businesses
- The European Commission and/or national regulators should announce an enforcement delay